INSTITUTO NACIONAL DE CIBERSEGURIDAD

“Aprendiendo ciberseguridad en tiempos de confinamiento”

Ruth García Ruiz

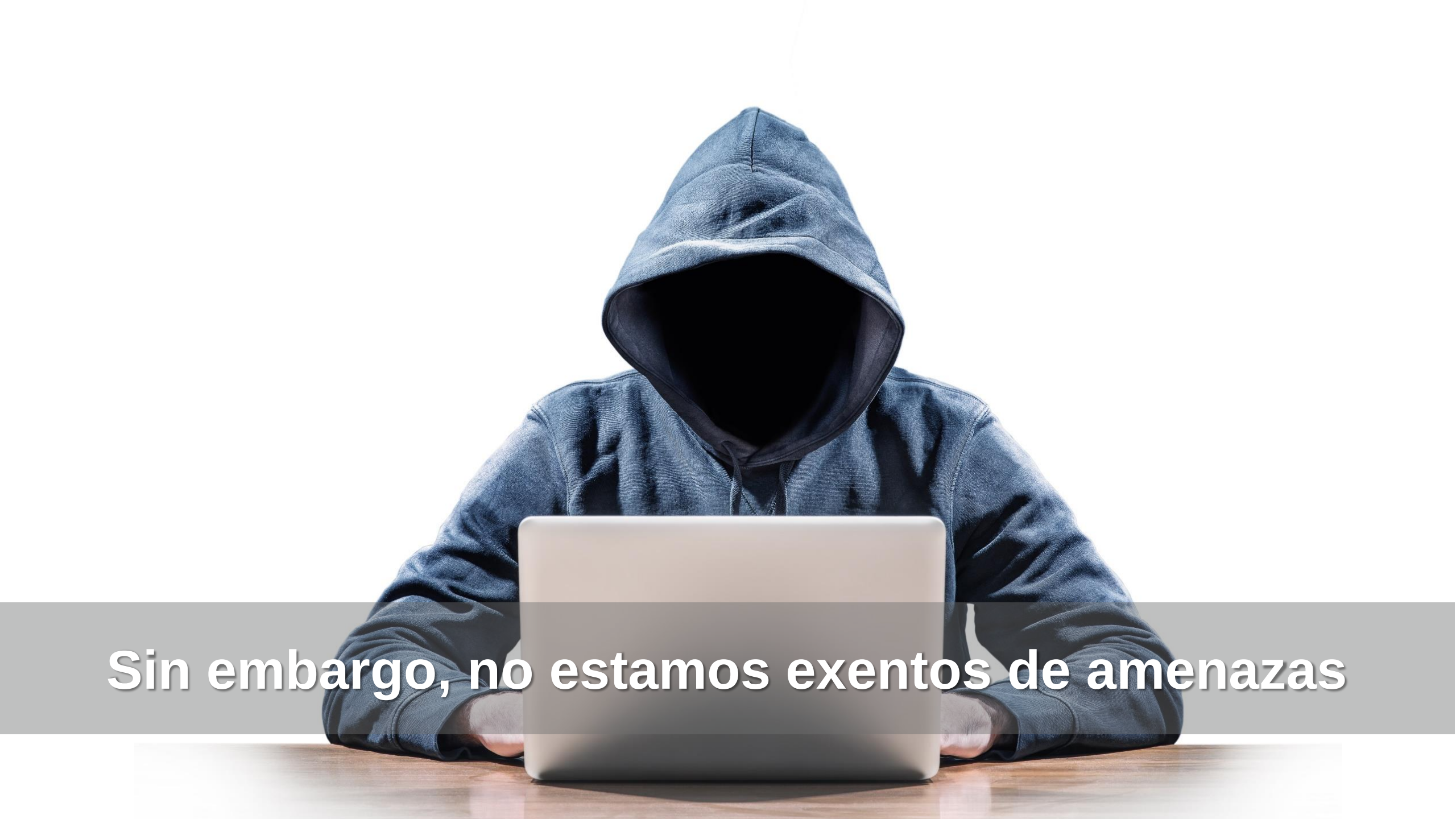
GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

017 TU AYUDA EN CIBERSEGURIDAD incibe_

Pongámonos en contexto antes de empezar

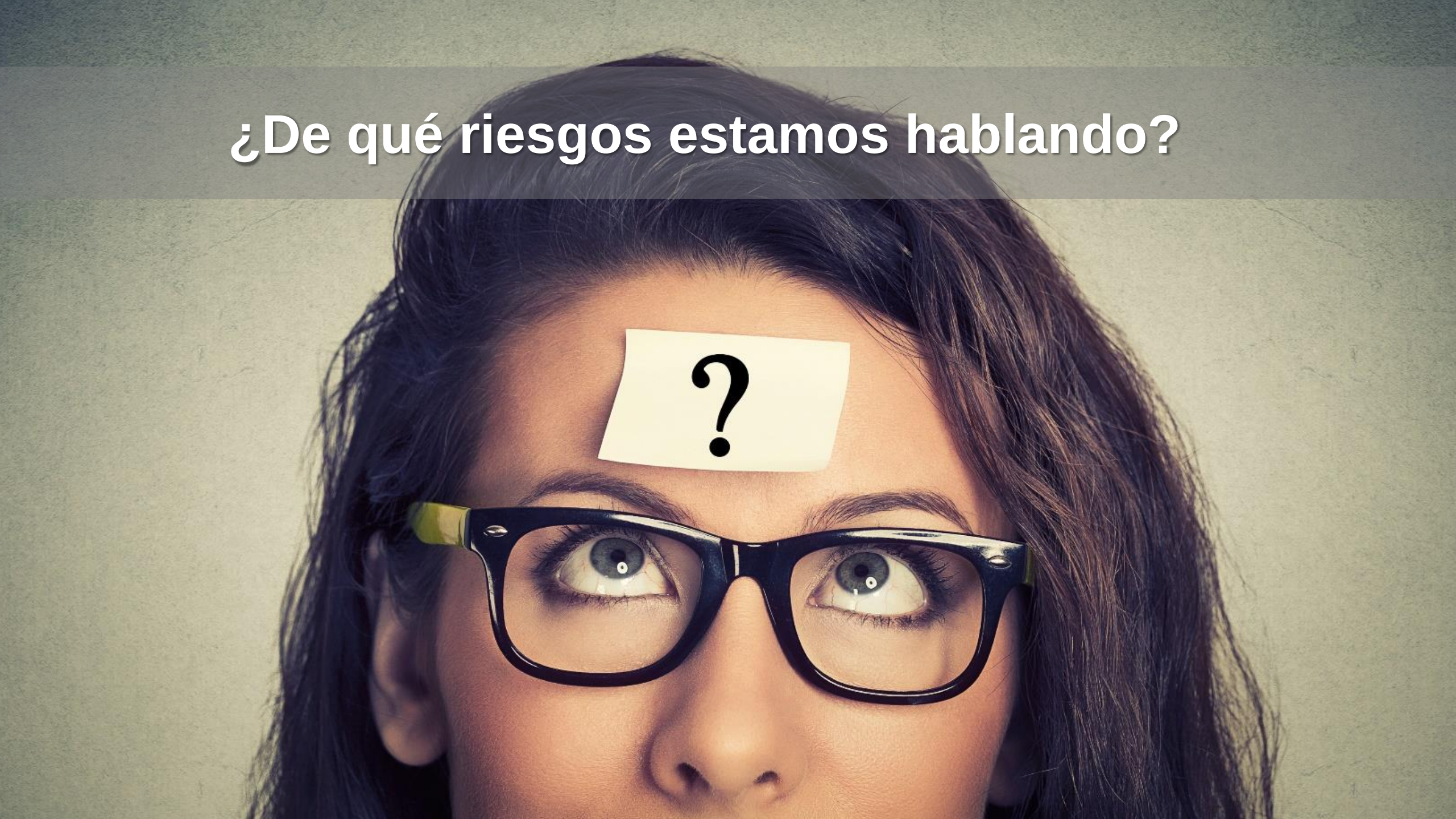
Vivimos en una sociedad digital hiperconectada

Aparentemente todo son beneficios



Sin embargo, no estamos exentos de amenazas

¿De qué riesgos estamos hablando?




¡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?

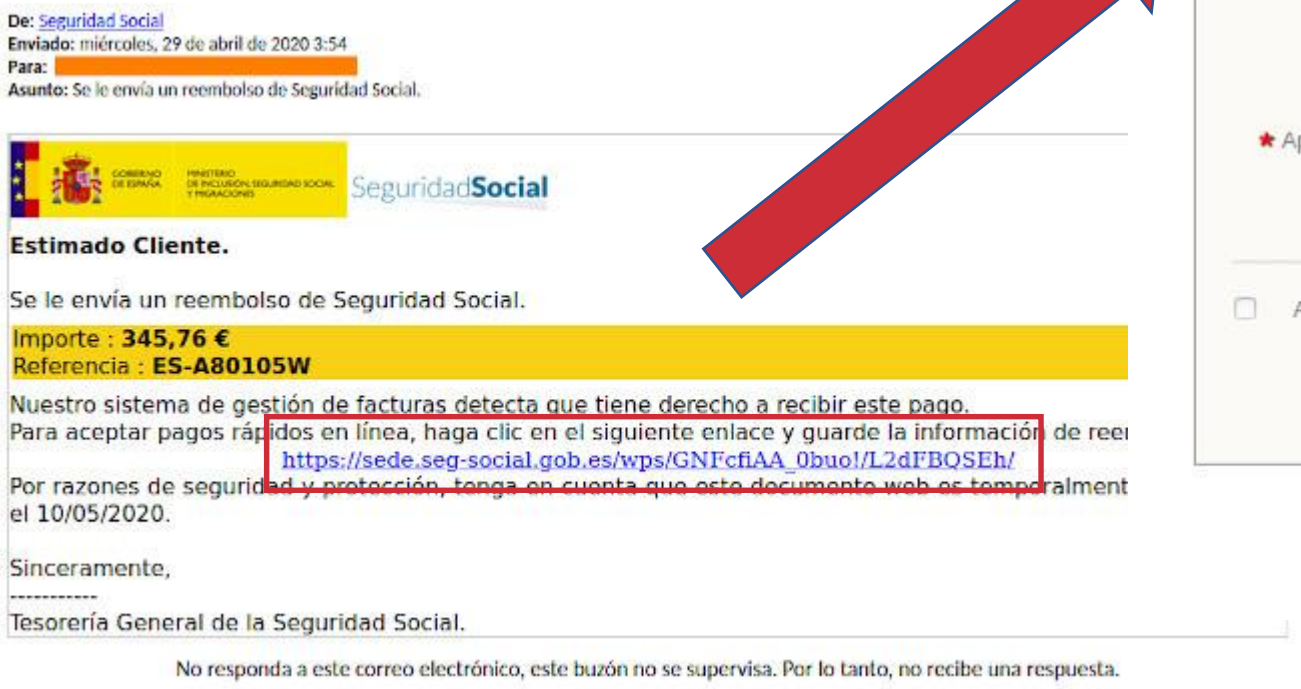
- Cómo evitar virus, fraudes y desinformación
- Cómo preparar un entorno de teletrabajo seguro
- Cómo proteger nuestra privacidad, identidad digital y reputación online

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.

Phishing



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

SeguridadSocial

Estimado Cliente.

Se le envía un reembolso de Seguridad Social.

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

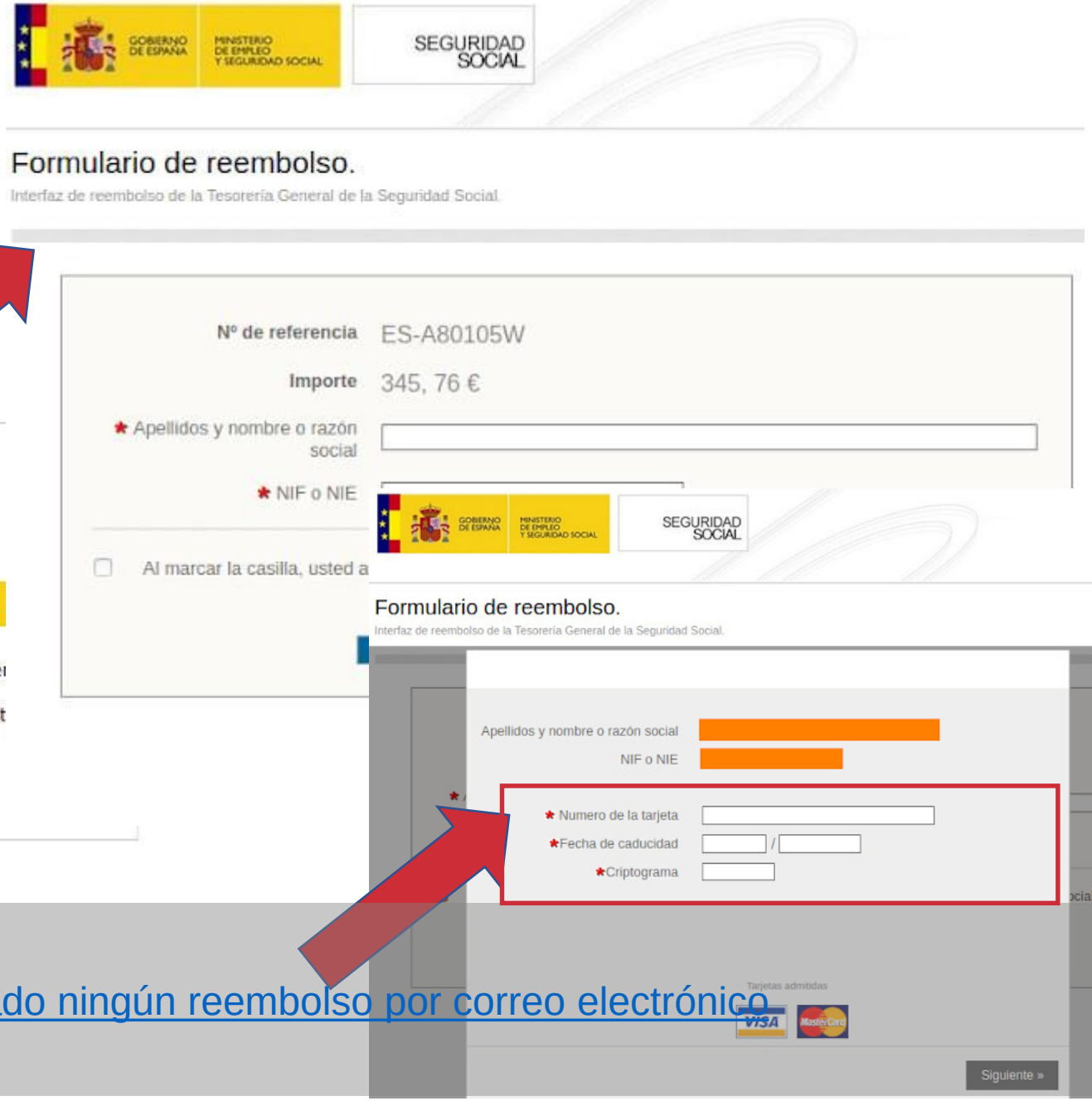
Nuestro sistema de gestión de facturas detecta que tiene derecho a recibir este pago.
Para aceptar pagos rápidos en línea, haga clic en el siguiente enlace y guarde la información de reembolso:
https://sede.seg-social.gob.es/wps/GNFcfiAA_0buo!/L2dFBQSEh/

Por razones de seguridad y protección, tenga en cuenta que este documento web es temporalmente válido hasta 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.



SEGURIDAD SOCIAL

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

SEGURIDAD SOCIAL

Formulario de reembolso.

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

Apellidos y nombre o razón social [redacted]

NIF o NIE [redacted]

* Numero de la tarjeta

*Fecha de caducidad /

*Criptograma

Tarjetas admitidas

Siguiente »

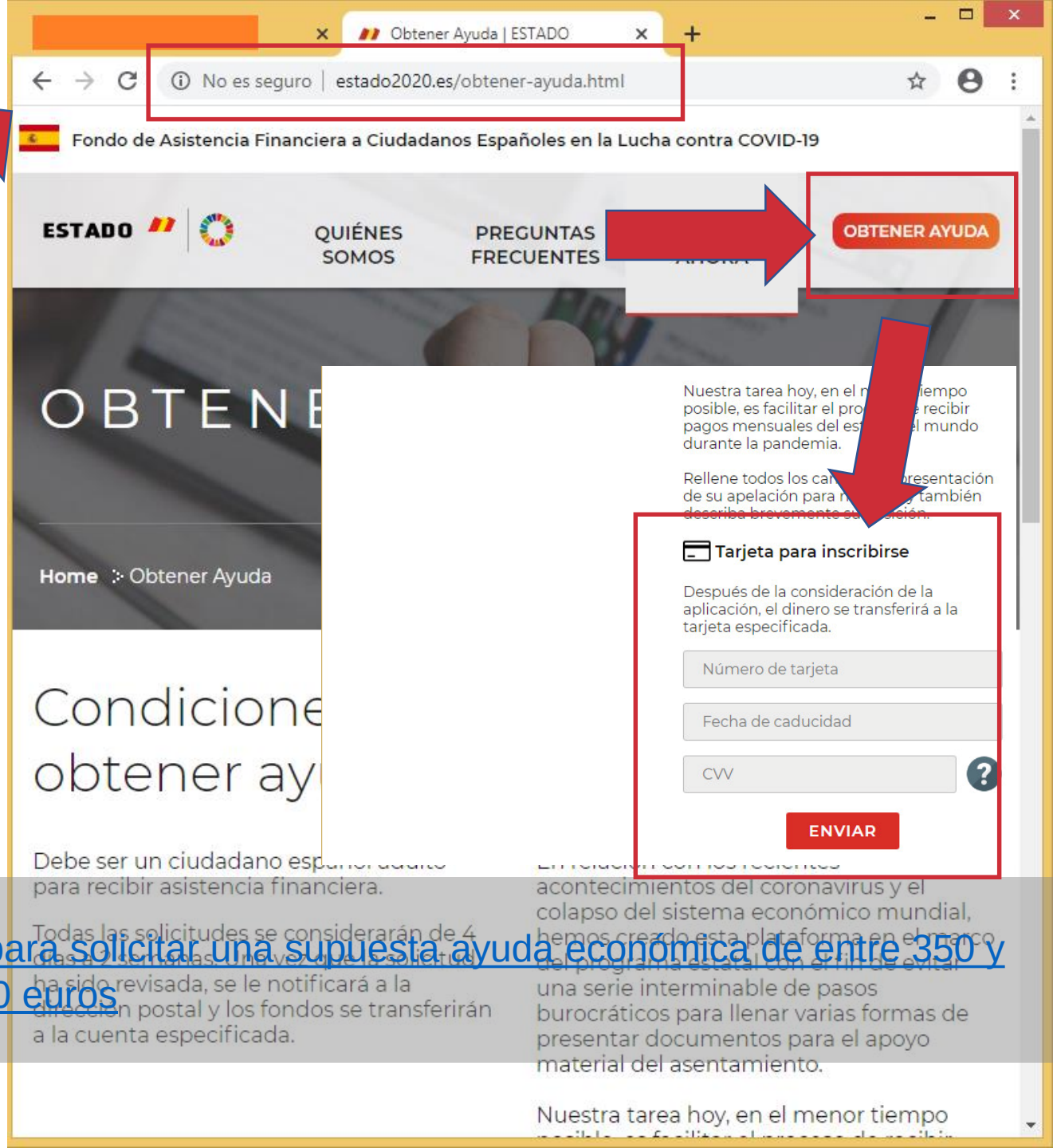
La Seguridad Social no te ha enviado ningún reembolso por correo electrónico

Smishing

13:23

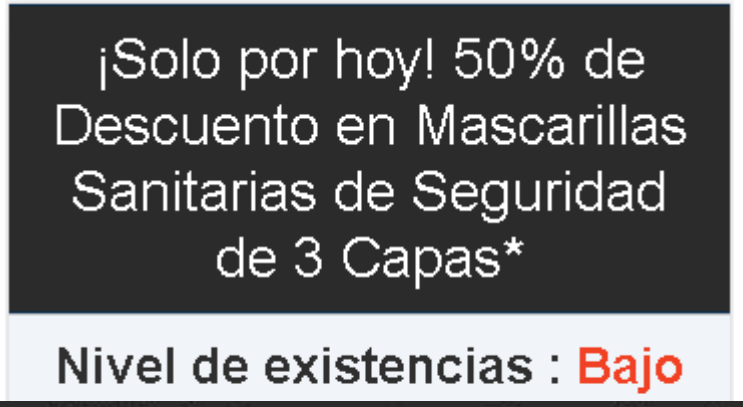
Hola, en relacion con la pandemia COVID19, el Estado destina 350-700 euros a sus ciudadanos.

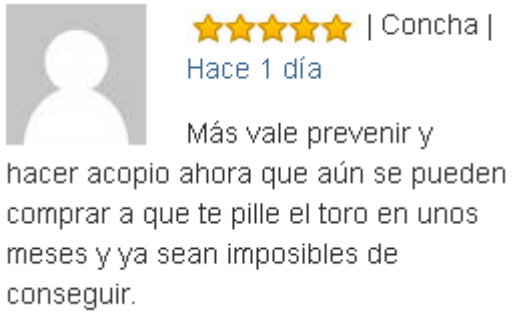
https://[redacted]20.es



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

Páginas fraudulentas





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

Malware

Realize el test de autoevaluacion Covid19 http://xxxxxxxxxxx.net

[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.

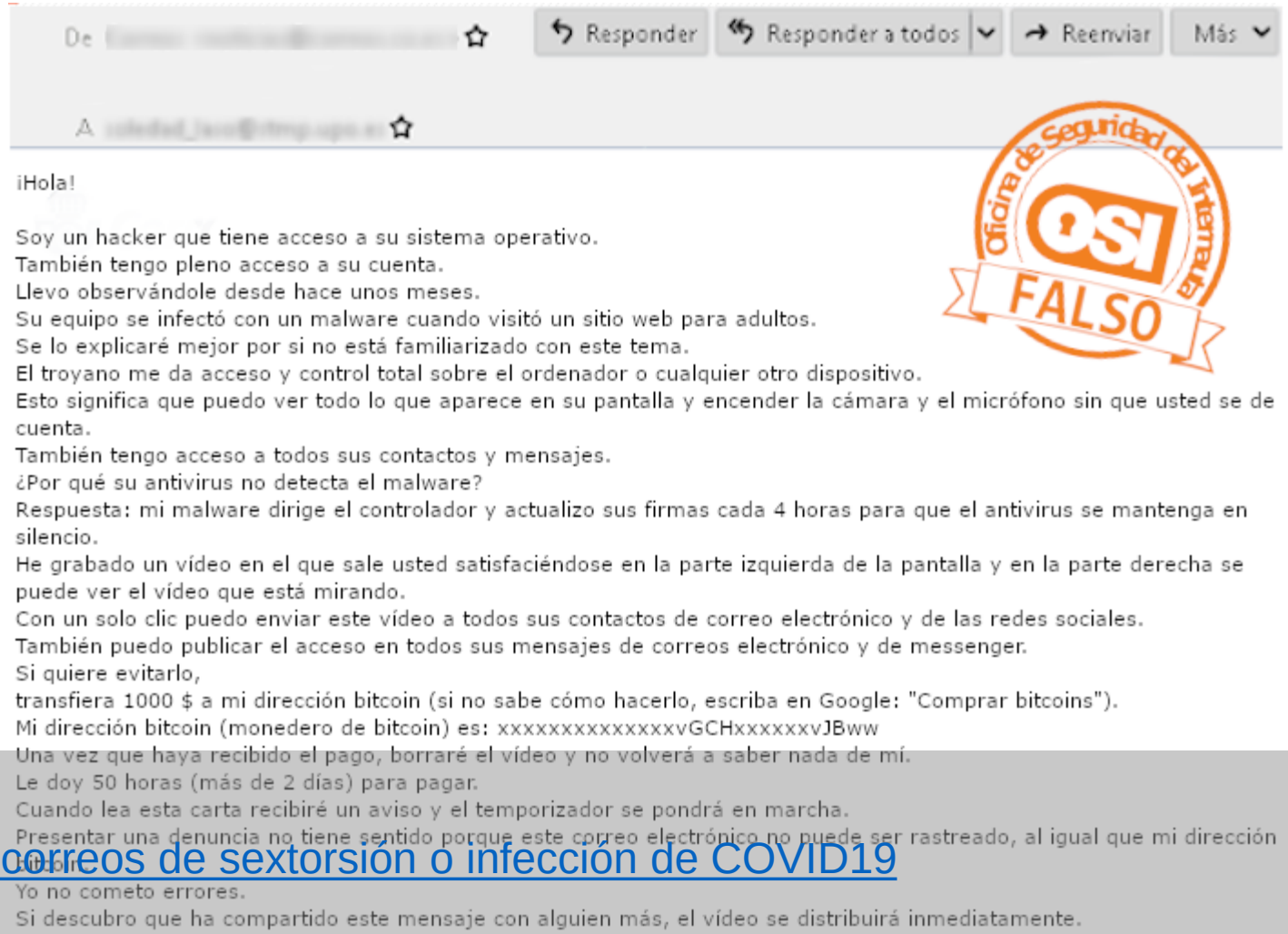
Dichas apps aseguran tener la utilidad de facilitar un mapa para seguir la evolución del coronavirus.

[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.



[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

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?

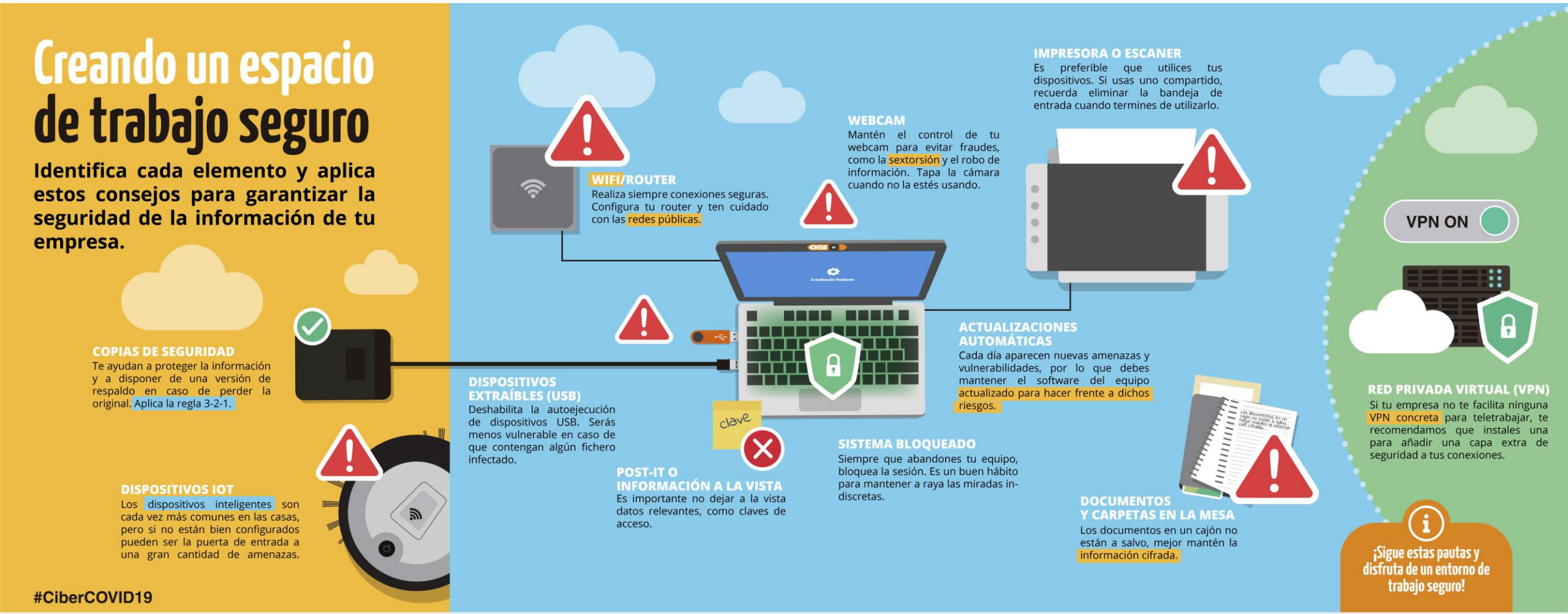
¿Te toca teletrabajar?

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.

WIFI/ROUTER
Realiza siempre conexiones seguras. Configura tu router y ten cuidado con las redes públicas.

WEBCAM
Mantén el control de tu webcam para evitar fraudes, como la sextorsión y el robo de información. Tapa la cámara cuando no la estés usando.

IMPRESORA O ESCANER
Es preferible que utilices tus dispositivos. Si usas uno compartido, recuerda eliminar la bandeja de entrada cuando termines de utilizarlo.

DISPOSITIVOS EXTRAÍBLES (USB)
Deshabilita la autoejecución de dispositivos USB. Serás menos vulnerable en caso de que contengan algún fichero infectado.

POST-IT O INFORMACIÓN A LA VISTA
Es importante no dejar a la vista datos relevantes, como claves de acceso.

ACTUALIZACIONES AUTOMÁTICAS
Cada día aparecen nuevas amenazas y vulnerabilidades, por lo que debes mantener el software del equipo actualizado para hacer frente a dichos riesgos.

SISTEMA BLOQUEADO
Siempre que abandones tu equipo, bloquea la sesión. Es un buen hábito para mantener a raya las miradas indiscretas.

DOCUMENTOS Y CARPETAS EN LA MESA
Los documentos en un cajón no están a salvo, mejor mantén la información cifrada.

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!

#CiberCOVID19

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
017

Mantente al día con nuestras campañas de concienciación para estar informado.
¡Es nuestra mejor defensa!
www.incibe.es | www.osi.es

OSI Oficina de Seguridad del Internauta
@osiseguridad osiseguridad

Pon a punto tu dispositivo para trabajar con él

Instala una herramienta antivirus

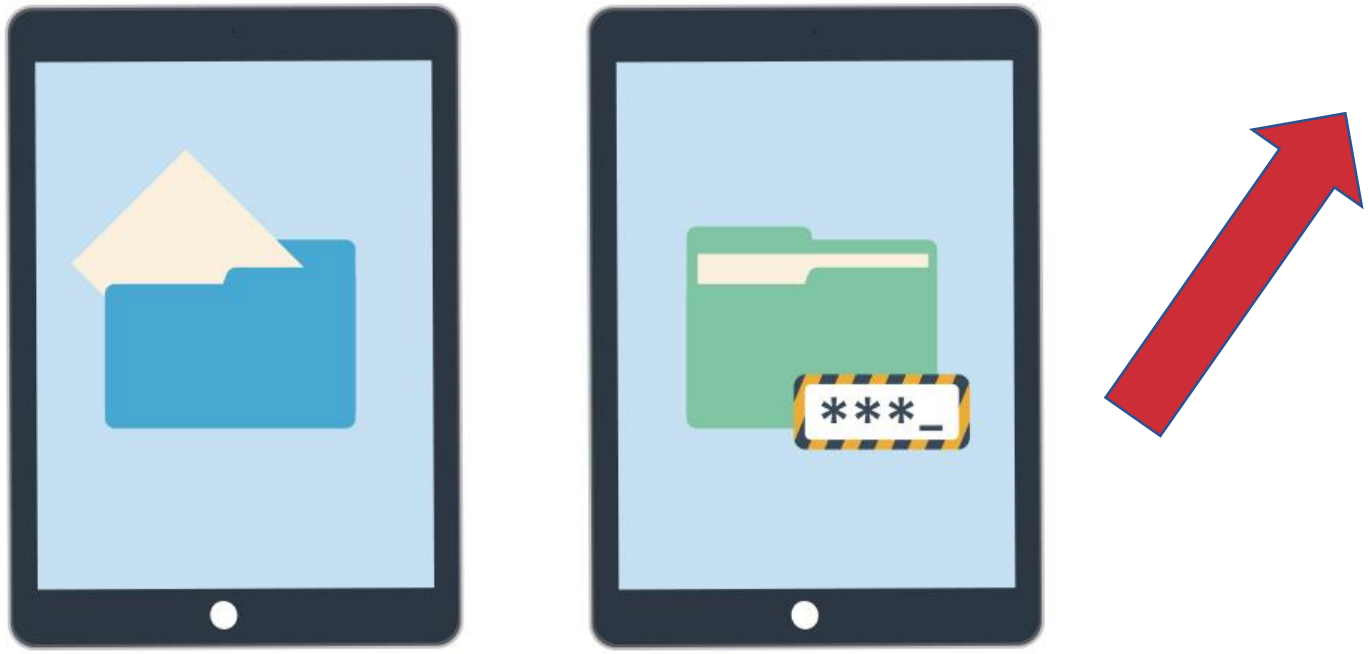
Actualiza el sistema operativo así como el resto de programas

Crea una cuenta de usuario diferente

Instala un Red Privada Virtual (VPN)

Haz copias de seguridad

Cifra la información

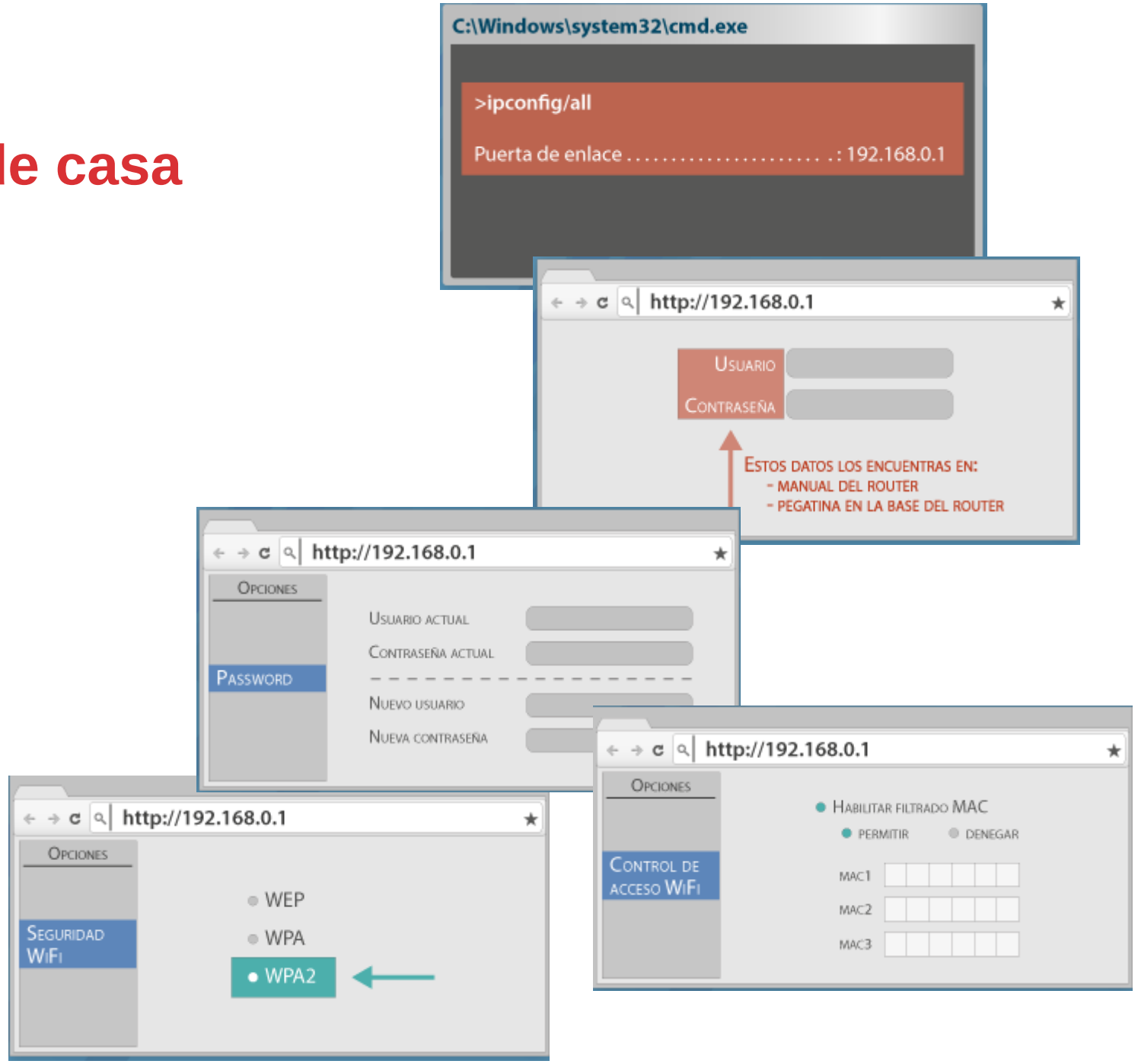


- Utiliza alguna herramienta específica. Ej: VerCrypt
- Apóyate en las opciones que incluyen los distintos sistemas operativos:
  - Windows 10: BitLocker
  - MAC OS: FileVault
  - iOS: cifrado por defecto.
  - Android: cifrado por defecto version 6 o superior. Adiantum para versions inferiores.

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

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?

¿Cuánta información existe sobre ti en Internet?

¿Tienes una identidad digital positiva?

¿Configuras adecuadamente tus perfiles?

¿Quiénes son tus contactos online?


¿Conoces los riesgos asociados al sexting?


We Are
here to
—help—

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

Oficina de Seguridad del Internauta

www.osi.es

consultas@osi.es

@osiseguridad

Oficina de Seguridad del Internauta

Información y actualidad

Avisos de seguridad

Blog

Historias reales

Campañas de concienciación temáticas

Los ciberdelincuentes, ¿quiénes son?

Dispositivos móviles

IoT, los riesgos de un mundo hiperconectado

Redes Sociales

¡Contraseñas seguras!

Oficina de Seguridad del Internauta

Servicios de soporte

OSI Oficina de Seguridad del Internauta
Servicio ANTIBOTNET

Conan mobile

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

¿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

017 TU AYUDA EN CIBERSEGURIDAD incibe_