

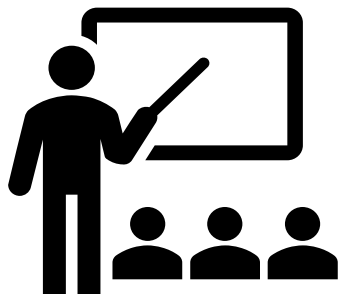
Las TIC y la seguridad dentro del marco docente

Año de realización: 2021

PROFESOR/A
Marco Antonio Lozano Merino



Índice. ¿Qué vamos aprender hoy?



- ▶ Reconociendo y saber cómo evitar virus, fraudes y desinformación (bulos, fake news) que circulan por Internet.
- ▶ Medidas básicas de ciberseguridad para proteger los dispositivos (pc, smartphones y tablets).
- ▶ Cómo proteger la privacidad, identidad digital y reputación online.

Pongámonos en contexto antes de empezar





Vivimos en una sociedad digital
hiperconectada



Aparentemente todo
son beneficios

A person wearing a dark blue hoodie is sitting at a wooden desk, working on a silver laptop. The person's face is obscured by a large, semi-transparent white speech bubble that contains the text. The background is white, and there are green geometric shapes on the left and right sides of the image.

Sin embargo, no
estamos exentos de
amenazas



¿De qué riesgos
estamos
hablando?

Virus, fraudes y desinformación en la Red

Vamos a investigar antes de continuar (10')



- ▶ ¿Qué técnicas utilizan los ciberdelincuentes para engañar a los usuarios?
- ▶ ¿Cómo preparan los ataques?
- ▶ ¿Cuáles creéis que son los más efectivos? ¿Por qué?

¿Qué es la ingeniería social?

Técnica usada por los ciberdelincuentes que consiste en engañar o manipular a las personas para conseguir su información personal o para obtener acceso a sus equipos.



¿Cómo consiguen engañarnos?

- ▶ Phishing
- ▶ Smishing
- ▶ Baiting
- ▶ Vishing
- ▶ Shoulder surfing
- ▶ Sextorsión
- ▶ Dumpster diving
- ▶ Quid pro quo
- ▶ Redes sociales

Técnicas de ingeniería social
¿Cómo consiguen engañarnos?

Pretexting
Base de cualquier ataque de ingeniería social.
Consiste en elaborar un escenario ficticio, donde el atacante tratará de que la víctima comparta información que, en circunstancias normales, no revelaría.

Sextorsión
Chantaje online amenazando a la víctima con difundir supuestamente contenido comprometedo de esta a sus contactos aunque no exista dicho contenido, si no accede a las peticiones, generalmente a realizar un pago.

Phishing
Busca "pescar" víctimas.
Generalmente se emplean correos electrónicos con archivos adjuntos infectados o links a páginas fraudulentas con el objetivo de tomar el control de sus equipos y robarles información confidencial.

Baiting
Emplea un cebo con software malicioso a la vista de sus víctimas para que ellos mismos infecten sus dispositivos.

Smishing
Se trata de una variante del "phishing", pero que se difunde a través de SMS.
Se pide al usuario que llame a un número de tarificación especial o que acceda a un enlace de una web falsa.

Vishing
Llamadas telefónicas donde el atacante se hace pasar por una organización/persona de confianza para que la víctima revele información privada.

Shoulder Surfing
Consiste en mirar por "esquina del hombro" al usuario buscando con observar lo que escribe o tiene en pantalla otro usuario para obtener información muy útil.

Quid pro quo
Prometen un beneficio a cambio de información personal y suelen ser compensaciones en forma de regalo, merchandising, dinero o acceso gratuito a programas de pago.

Dumpster diving
Se refiere al acto de "hojear en la basura", para obtener documentos con información personal o financiera.

Redes Sociales
Los ataques de ingeniería más comunes a través de las redes sociales son: freecitas, misas, descuentos, regalos y concursos, donde crees que puedes ganar algo.

incibe INSTITUTO NACIONAL DE CIBERSEGURIDAD
@INCIBE @INCIBE INCIBE
www.incibe.es | www.osi.es

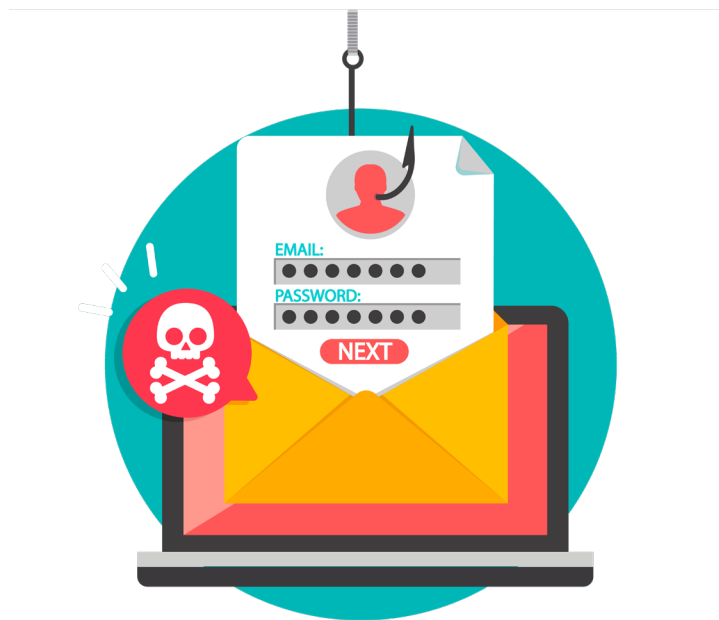
OSI Oficina de Seguridad del Internauta
@osiguridad @osiguridad osiguridad



¿Cómo preparan el engaño?



El correo electrónico es uno de los canales más utilizados



Cómo identificar correos maliciosos

- ▶ Remitente
- ▶ Asunto
- ▶ Objetivo del mensaje
- ▶ Redacción
- ▶ Enlaces
- ▶ Adjuntos



Phishing (I)

De: Seguridad Social
Enviado: miércoles, 29 de abril de 2020 3:54
Para: [Redacted]
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/

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.

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

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



Siguiente »

BY NC SA

Phishing (II)

De Amazon Prime <info@raankapao.com> ☆
Asunto: **Hola** **OBTENER UNA UN AÑO SUSCRIPCIÓN SOLO PARA €2.**
A info@raankapao.com ☆



Hola

COMPLETA EL QUESTIONARIO Y OBTENER UNA UN AÑO SUSCRIPCIÓN SOLO PARA €2.

Gratuita para todos Una selección de los mejores títulos, de forma gratuita para todos los clientes recién firmados.

No te pierdas esta oferta fantástica.



prime video

UN AÑO SUSCRIPCIÓN SOLO PARA €2

Suscripción de 1 año en

Nombre Apellido

Dirección

Ciudad Código postal

Teléfono

Email

SEGUIR

1 año de suscripción solo para €2.

Fraudes por 2€. Detectada suplantación de marcas conocidas ofreciendo sus servicios a bajo coste
Ve todo lo que quieras desde todos tus dispositivos



Phishing (III)

De Correos : centro de ayuda <support@Correos.net.es> ☆
Asunto **RE : Envío número 1-ES196 **** 726 !**



Envío número 1-ES196 **** 726 todavía no ha podido ser entregado por el motivo: Dirección incorrecta

Intento de entrega fallido : 26 de Agosto de 2020 , 16:38.
Entrega prevista : 27 de Agosto de 2020 , 10:00 - 14:00.

Para recibir su paquete mañana, nos envíe su dirección correcta y pague los nuevos costos de envío (1,40 €) en el siguiente enlace

[COMPLETE MI DIRECCIÓN DE ENTREGA](#)

Importante :

También puede elegir un punto de recogida para recuperar su paquete.
complete su dirección antes 23:59 Para recibir su paquete mañana.officers

FECHA 15/07/2020

PASO 1 : PAGO DE GASTOS DEL NUEVO INTENTO DE ENTREGA

IMPORTE : 1,16 €

MÉTODO DE PAGO :
TARJETA

PAGAR Y CONTINUAR

CANCELAR

Redsys

Correos

1 Selección método de pago 2 Comprobación autenticación 3 Solicitando Autorización 4 Resultado Transacción

Datos de la operación

Importe: **1,16 €**

Comercio: SOCIEDAD ESTATAL (CORREOS)

Terminal: 346841091-1

Pedido: 11196298004

ServiRed

Pagar con tarjeta

Nº Tarjeta:

Caducidad: mm aa

Cód. Seguridad: ?

PIN de Cajero:

Cancelar Pagar

Seguridad en el marco docente

Phishing a Correos solicitando un pago de 1,99€



Phishing (IV)

De Amazon.com.es <shipment-tracking@amazon.com.es> ☆
Asunto **Comprobante Fiscal Digital - 701-7450617-3626639 de 4 productos (812501)** 4:10
A isabel_smaer@gmpt.upct.es ☆



De Notificacion <contato@acesso financeiro.com> ☆
Asunto **Fwd: factura pendiente - Nº (733012)** 6:58
A [redacted] ☆

De Administracion Tributaria <impuestos@hacienda.gob.es>
Asunto **Notificacion Pendiente.. - [id 821144356]**
A [redacted] ☆



[Descargar todo como.zip archivos adjuntos \(128 k](#)

se anexa el siguiente comprobante fiscal digital

Remitente: Servicio de Administración Tributaria.

Hemos identificado que tienes pendiente de presentar, al 23 de

A quien corresponda

SERIE Y FOLIO:

FECHA DE EMISION:

MONTO TOTAL:

2158945

23/07/2020

6435.20 24/07/2020 01:43:16

Hola,

Tu paquete con 4 productos se entregará el 22/07

Se anexa el siguiente comprobante fiscal digital en su formato.

HTML:SAA031020IBA_Factura_8741_#701-7450617-3626639_de 4



[ver en el navegador](#)

Cordial Saludo,

Este email foi enviado para o endereço que não pode receber emails. Não responda este email.

Le recordamos que se **vinció el prazo de pagos de su factura** con nosotros, la factura **LALSJHDHD8282719941KKLD**.

Lamentamos informarle que **si el pago no se realiza hasta 30 de abril del 2020 suspenderemos los servicios y pasaremos su cuenta a nuestros abogados.**

[Descargar la factura.](#)

1 adjunto: HTMLSAA031020IBA_Factura_8741_#701-7450617-3626639_de 4_productos

© 2020 Vodafone España S.A.U.Avda. América 115, 28042 Madrid

Nuevos pretextos para descargar malware desde correos electrónicos

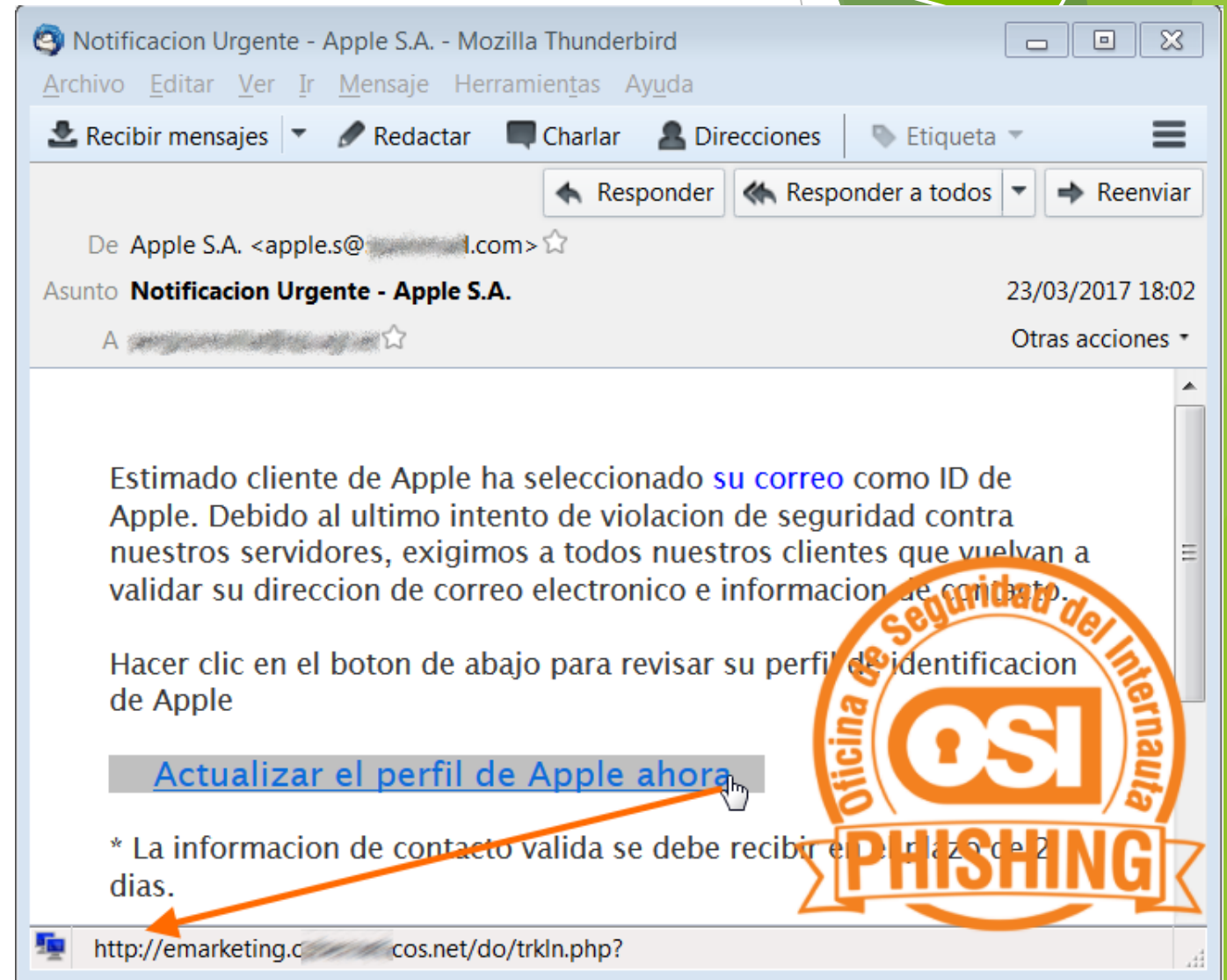
Guardar



MÁS SERVICIOS UTILIZADOS PARA PHISHING:

Seguridad en el marco docente

- Redes sociales: Facebook, Twitter, Instagram, TikTok, etc.
- Plataformas de videojuegos: PlayStation, Nintendo, Xbox, etc.
- Servicios de almacenamiento en la nube: Drive, Dropbox, etc.
- Servicios de correo electrónico: Gmail, Outlook, etc.
- Plataformas de entretenimiento: Netflix, HBO, Spotify, etc.
- Marketplaces: Amazon, eBay, etc.
- Etc.



OTROS CORREOS ELECTRÓNICOS FRAUDULENTOS

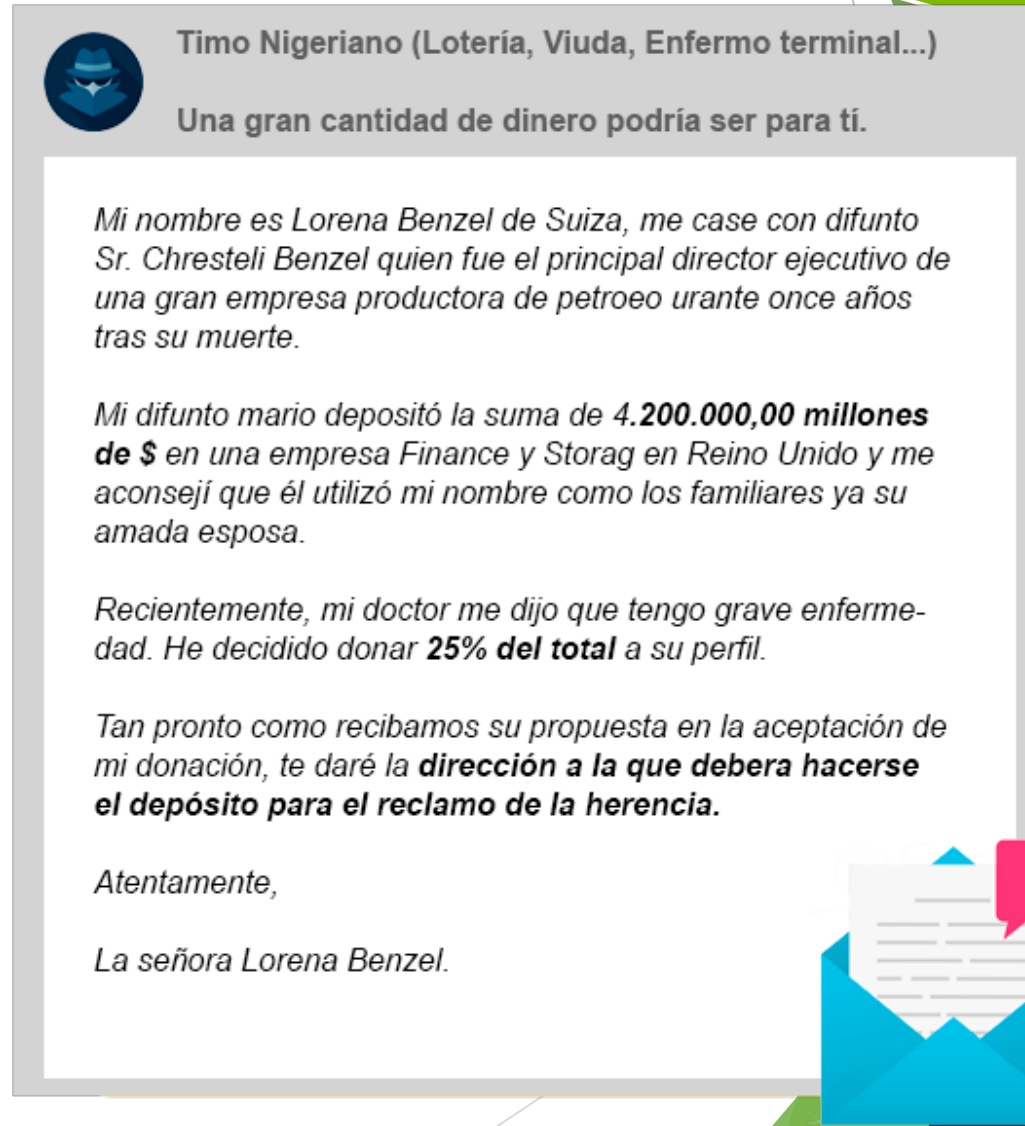
Seguridad en el marco docente



TIMO NIGERIANO (LOTERÍA, VIUDA, ENFERMO TERMINAL)

- ▶ Se basa en mostrarnos una oportunidad única en nuestra vida:

Seguridad en el marco docente



The image shows a screenshot of a scam message. At the top left is a profile picture of a person wearing a blue hooded mask. To the right of the picture is the name 'Timo Nigeriano (Lotería, Viuda, Enfermo terminal...)' and the text 'Una gran cantidad de dinero podría ser para ti.' Below this is a white box containing the main text of the scam, which is written in Spanish. The text describes a woman named Lorena Benzel who claims to be the widow of a man who worked for a large oil company. She says she has a large sum of money in a bank account in the UK and is offering to donate 25% of it to the recipient if they help her with the inheritance process. The message ends with 'Atentamente, La señora Lorena Benzel.' In the bottom right corner of the screenshot, there is a blue envelope icon with a white document inside and a pink exclamation mark icon above it. Below the envelope icon are two small circular icons: one with a dollar sign and a slash through it, and another with a dollar sign and a circle around it. Below these icons are the letters 'NC' and 'SA'.

Timo Nigeriano (Lotería, Viuda, Enfermo terminal...)
Una gran cantidad de dinero podría ser para ti.


Mi nombre es Lorena Benzel de Suiza, me case con difunto Sr. Chresteli Benzel quien fue el principal director ejecutivo de una gran empresa productora de petroeo urante once años tras su muerte.

*Mi difunto mario depositó la suma de **4.200.000,00 millones de \$** en una empresa Finance y Storag en Reino Unido y me aconsejé que él utilizó mi nombre como los familiares ya su amada esposa.*

*Recientemente, mi doctor me dijo que tengo grave enfermedad. He decidido donar **25% del total** a su perfil.*

*Tan pronto como recibamos su propuesta en la aceptación de mi donación, te daré la **dirección a la que debera hacerse el depósito para el reclamo de la herencia.***

Atentamente,
La señora Lorena Benzel.

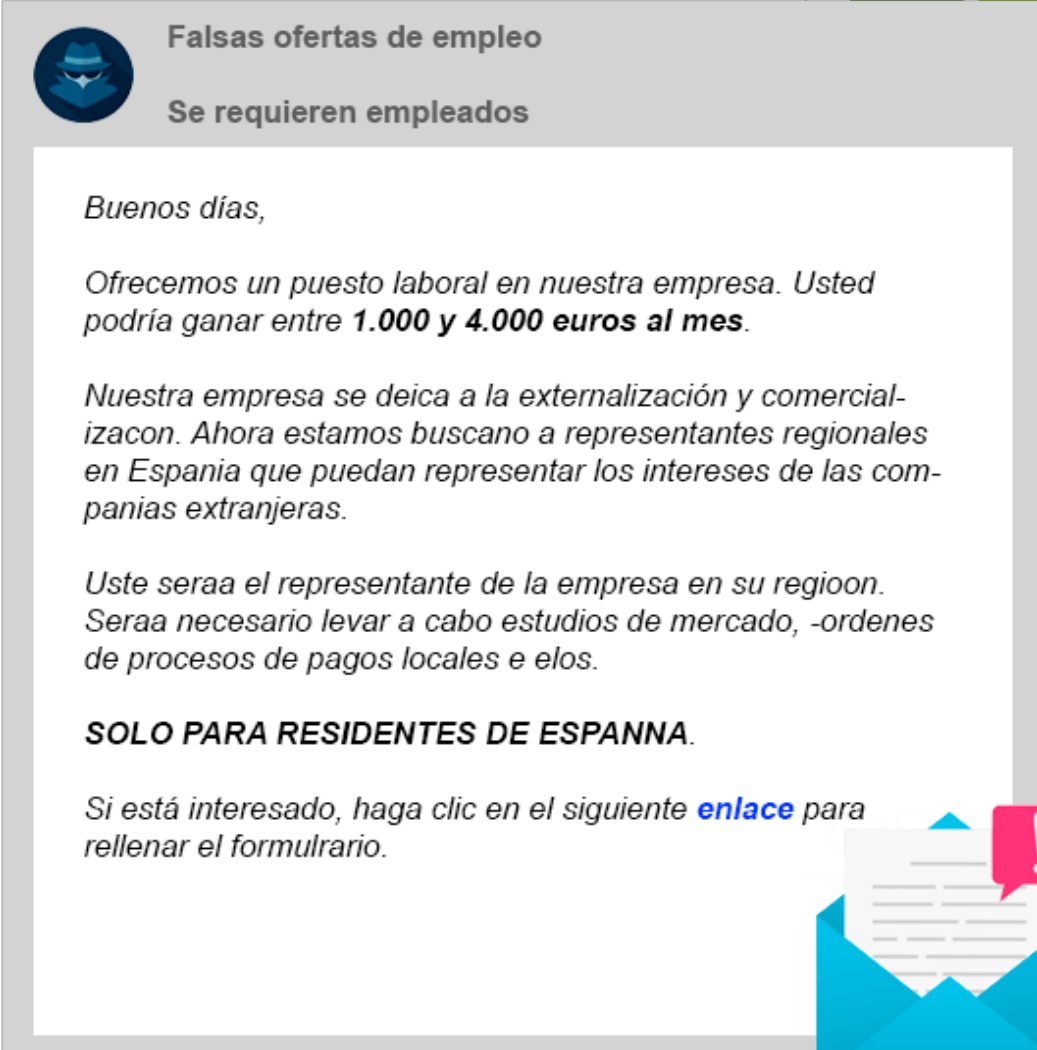


NC SA

FALSAS OFERTAS DE EMPLEO

- ▶ Los ciberdelincuentes se aprovechan de la necesidad de un empleo.

Seguridad en el marco docente



Falsas ofertas de empleo
Se requieren empleados

Buenos días,



*Ofrecemos un puesto laboral en nuestra empresa. Usted podría ganar entre **1.000 y 4.000 euros al mes.***

Nuestra empresa se deica a la externalización y comercialización. Ahora estamos buscano a representantes regionales en Espania que puedan representar los intereses de las companias extranjeras.

Uste seraa el representante de la empresa en su region. Seraa necesario levar a cabo estudios de mercado, -ordenes de procesos de pagos locales e ellos.

SOLO PARA RESIDENTES DE ESPANNA.

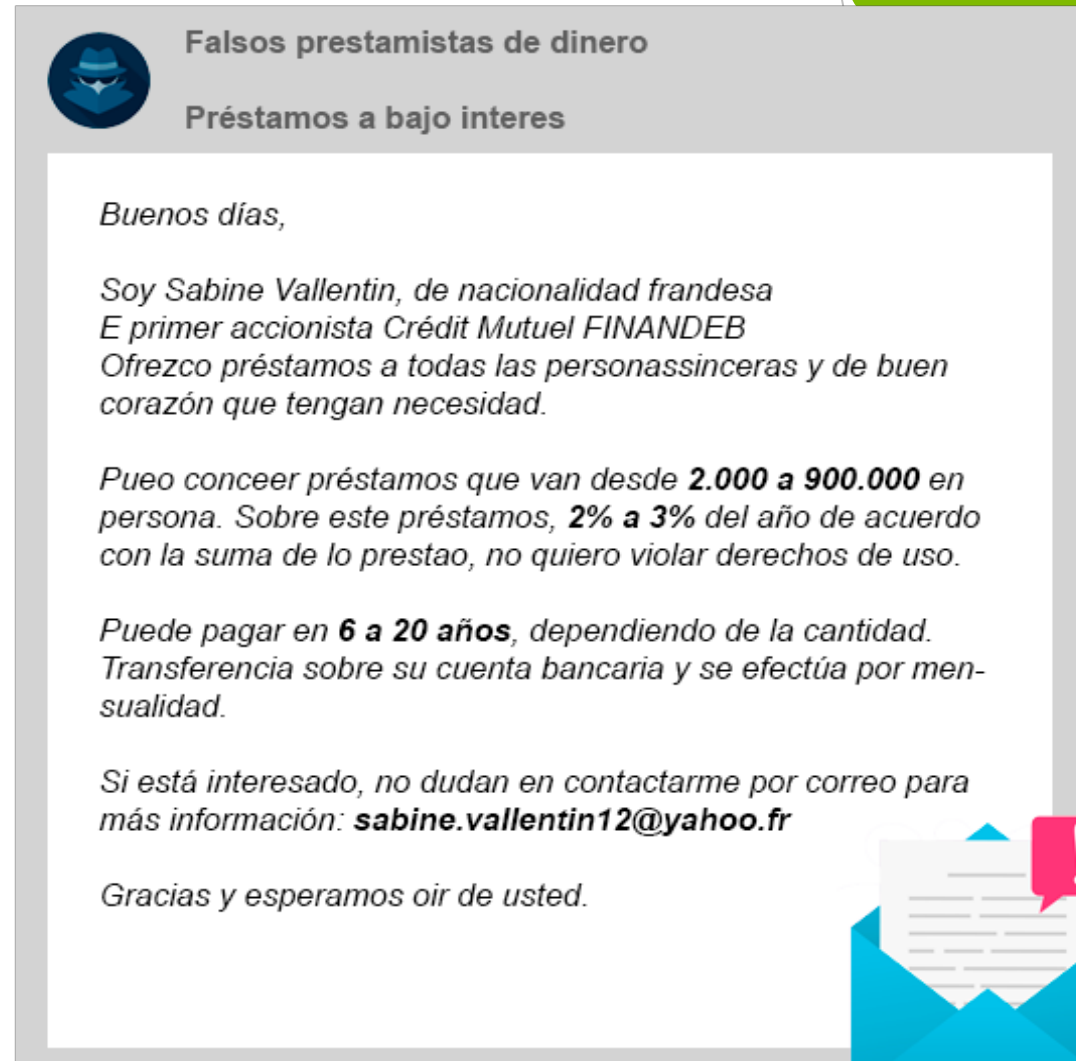
Si está interesado, haga clic en el siguiente [enlace](#) para rellenar el formulario.



PRESTAMISTAS FALSOS DE DINERO

Seguridad en el marco docente

- ▶ Los ciberdelincuentes se aprovechan de los apuros económicos.



Falsos prestamistas de dinero

Préstamos a bajo interes

Buenos días,

*Soy Sabine Vallentin, de nacionalidad frandesa
E primer accionista Crédit Mutuel FINANDEB
Ofrezco préstamos a todas las personassinceras y de buen
corazón que tengan necesidad.*

*Pueo conceer préstamos que van desde **2.000 a 900.000** en
persona. Sobre este préstamos, **2% a 3%** del año de acuerdo
con la suma de lo prestao, no quiero violar derechos de uso.*

*Puede pagar en **6 a 20 años**, dependiendo de la cantidad.
Transferencia sobre su cuenta bancaria y se efectúa por men-
sualidad.*

*Si está interesado, no dudan en contactarme por correo para
más información: **sabine.vallentin12@yahoo.fr***

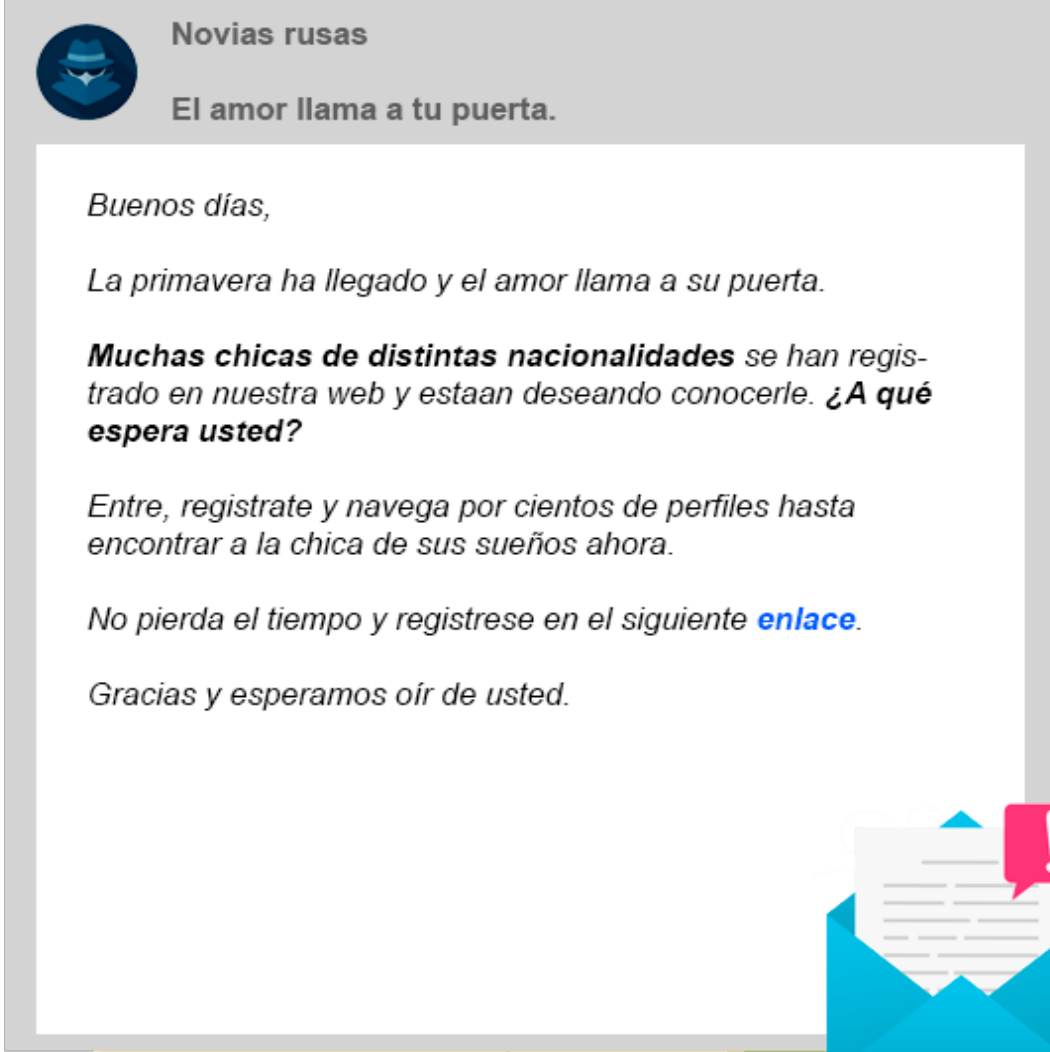
Gracias y esperamos oir de usted.



NOVIAS RUSAS

- ▶ El amor a través de Internet puede ser más engañoso de lo que nos gustaría.
- ▶ Este tipo de estafas se aprovechan de nosotros y nuestro interés en encontrar una media naranja.

Seguridad en el marco docente



Novias rusas
El amor llama a tu puerta.

Buenos días,



La primavera ha llegado y el amor llama a su puerta.

Muchas chicas de distintas nacionalidades se han registrado en nuestra web y estaan deseando conocerle. ¿A qué espera usted?

Entre, regístrate y navega por cientos de perfiles hasta encontrar a la chica de sus sueños ahora.

No pierda el tiempo y regístrese en el siguiente [enlace](#).

Gracias y esperamos oír de usted.



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.

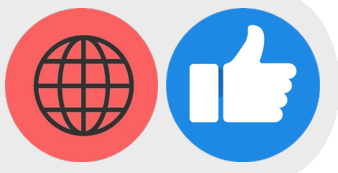
En ambos casos, el ciberdelincuente amenaza con hacer efectiva su extorsión si no se realiza el pago de una determinada cantidad en bitcoins.

Detectada oleada de falsos correos de sextorsión o infección de COVID19



RECOMENDACIONES Y CONSEJOS

- Captarán nuestra atención: con una oportunidad demasiado atractiva para ser verdad, con dinero fácil o una cantidad muy sustancial.
- La redacción de los mensajes suele estar llena de faltas de ortografía, errores gramaticales o una mala traducción del texto.
- Generalmente se referirán a nosotros de forma genérica o, en su defecto, con alguna prueba como un correo o contraseña nuestra con la que probar su mensaje, como es el caso de la sextorsión.
- En algún momento se nos pedirá dinero por adelantado o que compartamos con ellos información personal.



RECOMENDACIONES Y CONSEJOS

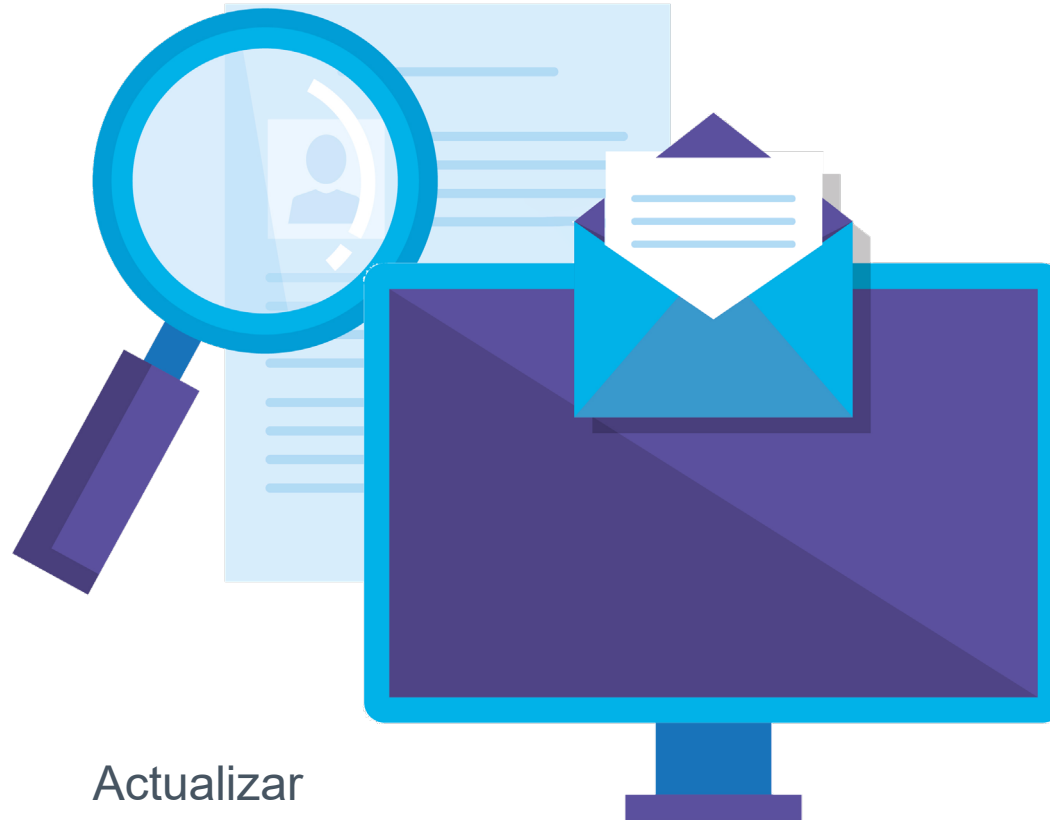
Seguridad en el marco docente

No responder

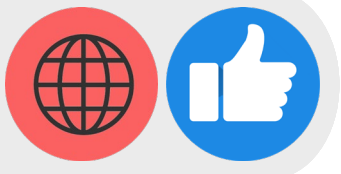
No descargar

No compartir información

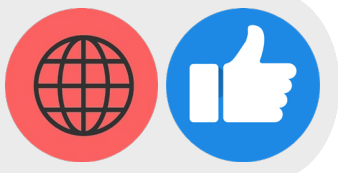
Ignorar enlaces



Actualizar



PHISHING EN 3 MINUTOS (PoC)

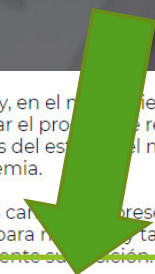
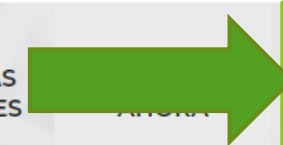


Smishing (I)

13:23

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

[https://\[redacted\].es](https://[redacted].es)



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

A screenshot of a web browser displaying a fraudulent website. The browser's address bar shows 'estado2020.es/obtener-ayuda.html' with a warning icon and the text 'No es seguro'. The website header includes the Spanish flag and the word 'ESTADO', along with navigation links for 'QUIÉNES SOMOS', 'PREGUNTAS FRECUENTES', and a prominent red 'OBTENER AYUDA' button. The main content area features the heading 'CONDICIONES PARA OBTENER AYUDA' and a registration form titled 'Tarjeta para inscribirse'. The form contains input fields for 'Número de tarjeta', 'Fecha de caducidad', and 'CVV', followed by a red 'ENVIAR' button. The text on the page describes a financial aid program for citizens during the COVID-19 pandemic, mentioning monthly payments and a review process.

Smishing (II)

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

The screenshot shows the official website for COVID-19 in Spain. A green box highlights a security warning: "No es seguro | autoevaluacion.net". A green arrow points from this warning to a button labeled "ENTENDIDO. REALIZAR AUTOEVALUACIÓN". Another green arrow points from the top right to a "Statistica" button. A third green arrow points from a table of cases to the "ENTENDIDO..." button. A fourth green arrow points from the "ENTENDIDO..." button to a list of links at the bottom.

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

CASOS TOTALES (PCR+) 218011

Casos últimas 24h (PCR+) 356

Recuperados 121343

Fallecidos 25428

Casos por CCAA

CCAA	Total	Ult.24h	Últ.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	2000	0	10.00
Comunidad de Madrid	62395	1	69.23

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

Statistica

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



Vishing

 **Ministerio Inclusión Seguridad Social Migraciones** @i... · 16 sept. · 17

¡¡OJO!! #NoPiques #estafa

⚠️ La #SeguridadSocial no utiliza la aplicación Bizum. Es un **TIMO**

!! RECORDAD: Cualquier gestión con la Seguridad Social o cualquier otro organismo de la Administración Pública ha de hacerse siempre a través de páginas oficiales

¡ALERTA!

Cuidado si te llama una persona y te dice que trabaja en la Tesorería General de la Seguridad Social y tienes que devolver dinero vía Bizum. **Es un timo.**



Estafa a través de llamadas telefónicas que suplantan a la Seguridad Social para realizar cargos a usuarios a través de un proveedor de servicios de pago (Bizum)

+34 [redacted]

Hola buenas noches mi nombre es [redacted] y soy asesora online de Bizum 23:22

Pregunto por [redacted] 23:22

Soy yo... 23:23 ✓✓

Me pongo en contacto con usted porque ha recibido un ingreso mediante bizum de 386 euros 23:23

Y al parecer lo tiene desactivado 23:23

A estas horas un asesor? 23:24 ✓✓

La entidad emisora es la TGSS en concepto de prestación por hijo a cargo 23:24

Nosotros estamos 365 días las 24 horas 23:24

La tesorería de la seguridad social?

Por bizum? 23:25 ✓✓

Cómo identificar llamadas fraudulentas

- ▶ Ante la mínima duda, no proporciones la información que te solicitan y finaliza la llamada.
- ▶ Realiza una búsqueda del número por Internet, es posible que esté identificado como fraudulento y obtengas más información.
- ▶ Acude a la fuente oficial para comprobar la veracidad de lo que te proponen.
- ▶ Si se trata de un fraude, bloquea el número para que no puedan volver a llamarte.
- ▶ Jamás actúes por impulso. Utiliza el sentido común y reflexiona.

Cómo reportar fraudes

- ▶ ¿Quieres reportar un fraude? ¿Necesitas ayuda?



RESPUESTA A INCIDENTES DE
CIBERSEGURIDAD
incibe-cert_

- ▶ incidencias@incibe-cert.es



TU AYUDA EN
CIBERSEGURIDAD
incibe_

- ▶ Teléfono gratuito y confidencial: 017

Páginas fraudulentas (1)



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

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

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

¡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

Seguridad en el marco de esta oferta



★★★★★ | 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.

Páginas fraudulentas (II)

Seguridad en el marco docente

A screenshot of a fraudulent website, 'vip.saletoy.top', which is a clone of the LEGO Home of the Brick site. The page shows a login form with fields for 'Please Log In' and 'Please Log In'. A certificate verification window is overlaid on the page, displaying the following information:

Certificado

General Detalles Ruta de certificación

Ruta de certificación

- DigiCert Baltimore Root
- Cloudflare Inc ECC CA-3
- sni.cloudflaressl.com

Ver certificado

Estado del certificado:

Certificado válido.

Aceptar

Forgot your password?



Páginas fraudulentas (III)

Envío y Ingrese o Regístrese

Embalar
Mercancía g
Mercancía e
Cuando el p
tercero. Nos

Tiempo De
En General,

Seguir Pec
Hacemos us
Información
Apellido
Nombre
Email

6. Exe
Peu imj

Iniciar sesión Crear cuenta

Dirección de email

Contraseña

Ha olvidado contraseña

 IDENTIFICARSE

Puede usar la cuenta de miembro para disfrutar de los siguientes servicios:

-  ¡CREA UNA CUENTA Y RECIBE UN CUPÓN
-  Verifique fácilmente el estado logístico de los pedidos
-  Conveniente operación de retorno
-  Conozca las promociones y nuevos productos de primera mano.

es seguir pedid
roblemático.
cancia. Permitin

Cómo identificar webs fraudulentas



“Me encontraba navegando por Internet, buscando un par de zapatos nuevos que comprar, cuando encontré una oferta estupenda.

Estaban un 40% más baratos que en la tienda oficial, y me decidí a comprarlos. La web parecía fiable, aunque ya han pasado dos meses desde que los pedí y aún no me han llegado.”



¿Cómo nos afectaría?



Observar el aspecto visual

Una web mal construida y poco atractiva puede ser debido a que se ha hecho con prisas y/o tratando de copiar el estilo de una tienda oficial.



Monitorizar opiniones

Antes de comprar un producto revisaremos las opiniones de otros usuarios haciendo una búsqueda por Internet.

Comprobar información legal empresa

El NIF de la empresa y otros datos como la razón social o los datos de contactos son necesarios para identificar a una tienda online fiable.

Fijarse en los precios

Deben hacernos sospechar los precios demasiado bajos con respecto a las tiendas oficiales o al precio de mercado.

Recomendaciones “Buenas prácticas del cibernauta”



Comprobar certificado SSL **ON**

Las tiendas online fiables tendrán una conexión segura por HTTPS y contarán con un certificado de seguridad.

Leer condiciones y políticas **GDPR**

Seamos conscientes de las condiciones del servicio que se nos está ofreciendo, así como de las políticas de privacidad de la plataforma. Esta información suele incluirse dentro del “Aviso legal” de la web, y debemos sospechar si no lo vemos por ningún lado.

\$ Analizar pagos permitidos

Evitaremos páginas que, aunque contengan los logos de muchos métodos de pago online, a la hora de la verdad solo permiten transferencias a depósitos y pagos con tarjeta.

★ Contrastar reputación en la red

Un rápido vistazo por Internet, buscando por el nombre de la empresa o del vendedor, nos dirá si nos encontramos ante una estafa o fraude.

REVISAR LA DIRECCIÓN WEB

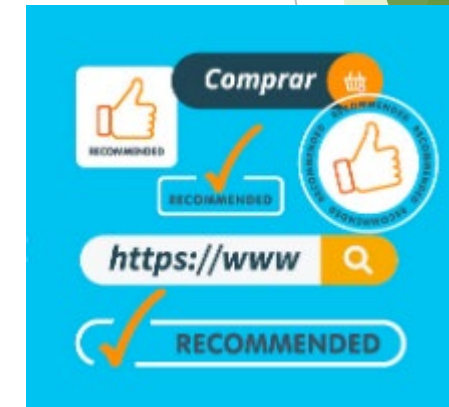
- La URL puede ofrecernos información muy útil:



HTTP / HTTPS



Certificado de seguridad



Sello de confianza

BUSCAR INFORMACIÓN SOBRE LA TIENDA

- ▶ Para valorar la reputación de una tienda:

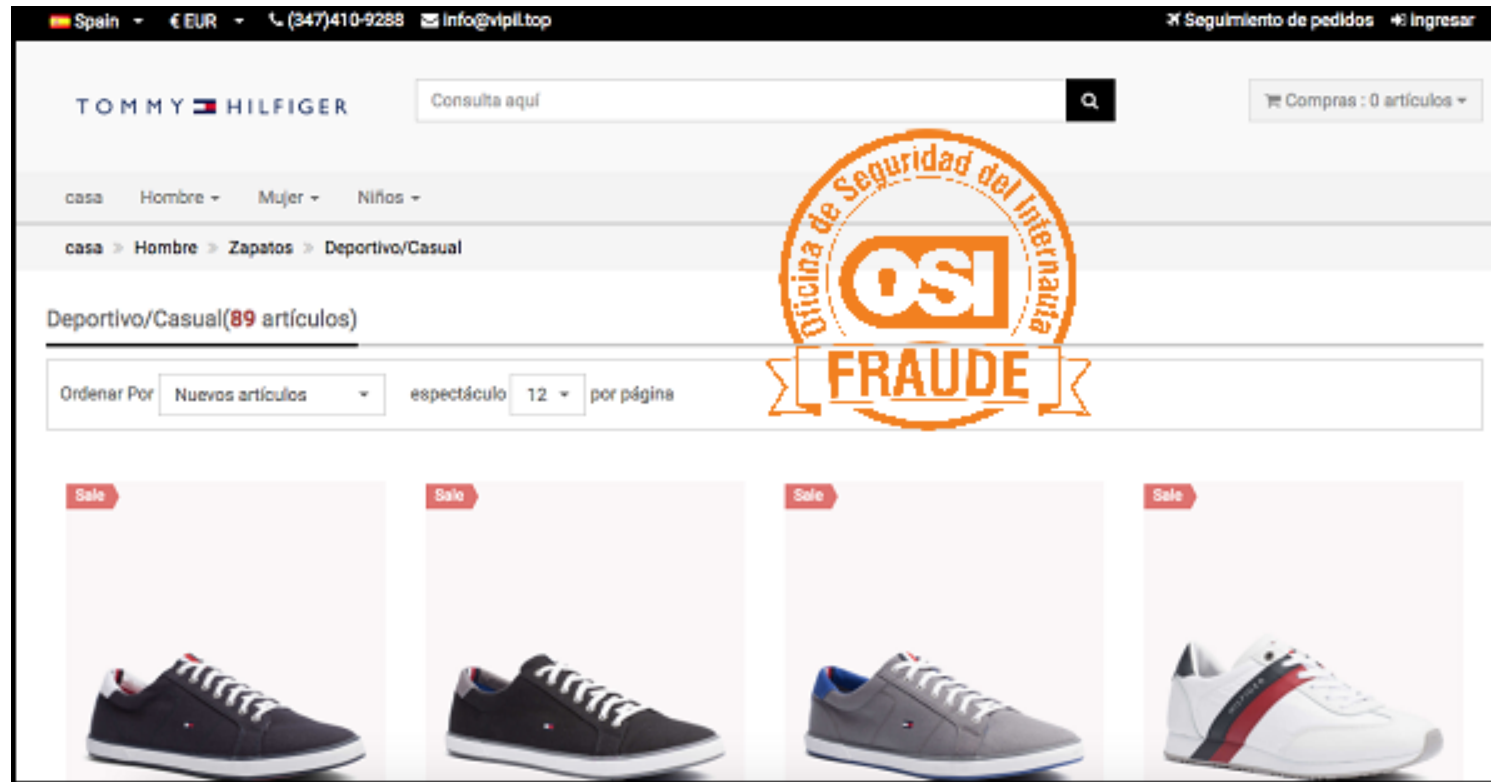


- ✓ Valoraciones de los usuarios.
- ✓ Búsqueda por Internet.
- ✓ Búsqueda de información legal.

REVISAR EL ASPECTO VISUAL DE LA TIENDA

Seguridad en el marco docente

- Un vistazo al diseño y elementos gráficos o visuales de la web nos puede ayudar:



COMPROBAR LOS PRECIOS

Seguridad en el marco docente

- También debemos comprobar los precios:



The advertisement shows three Ray-Ban sunglasses models. The first is a Wayfarer (RB2140F) with a price of €150.00 and a sale price of €19.99 (87% off). The second is an Aviator Classic (RB3025L) and the third is an Aviator Large Metal (RB3025 001/51 2N 58-14), both with a price of €150.00 and a sale price of €19.99 (87% off). A large orange watermark with a keyhole icon and the text 'Oficina de Seguridad del Internauta' and 'OSI' is overlaid on the Aviator models.

Modelo	Referencia	Precio Original	Precio de Venta	Descuento
RAY-BAN WAYFARER	RB2140F 901 54-18	€150.00	€19.99	87% OFF
RAY-BAN AVIATOR CLASSIC	RB3025L 2823 2N 58-14	€150.00	€19.99	87% OFF
RAY-BAN AVIATOR LARGE METAL	RB3025 001/51 2N 58-14	€150.00	€19.99	87% OFF

REVISAR LAS CONDICIONES DE ENVÍO Y DEVOLUCIÓN

Seguridad en el marco docente



Empresa en España



Empresa fuera de España

COMPROBAR LAS FORMAS DE PAGO

Seguridad en el marco docente



Tarjetas de crédito o débito



Tarjetas prepago



Transferencia bancaria



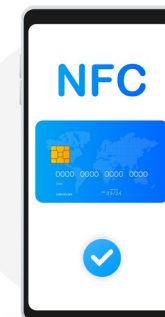
Plataformas de pago



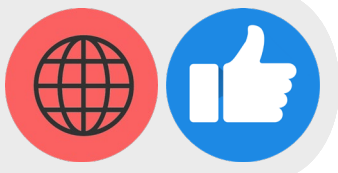
Transferencia instantánea



Pago contra reembolso



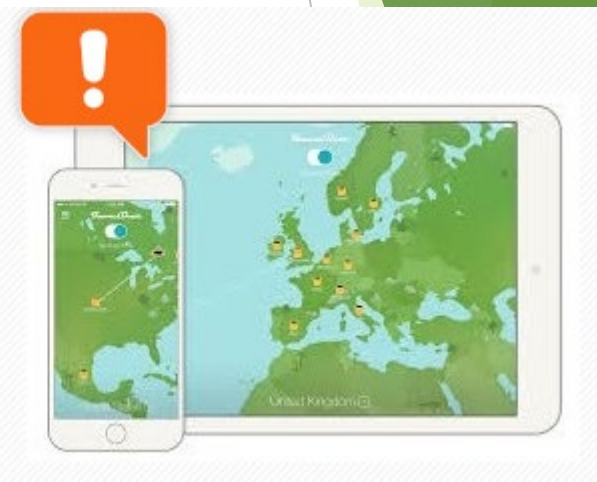
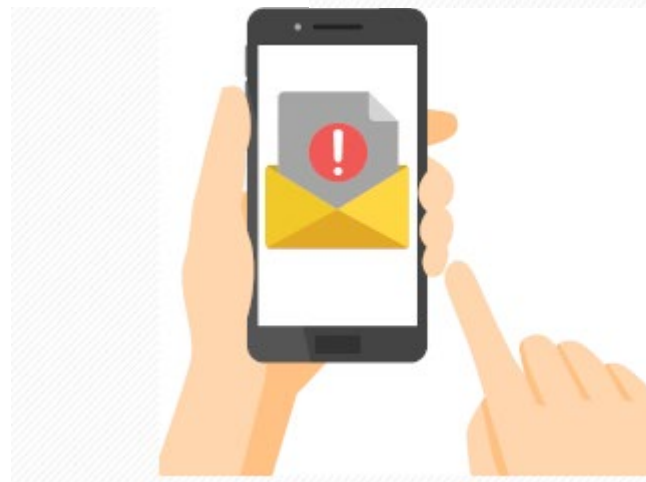
Pago con el teléfono móvil



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.

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



Seguridad en el marco docente

Detectadas aplicaciones maliciosas sobre la evolución del coronavirus

Cómo identificar apps fraudulentas

- 1. Comprobar quién es el desarrollador de la aplicación.** Si Pokemon Go es de Niantic, no debemos descargar la aplicación de otro desarrollador. Gran Hermano, es de Mediaset España, si descargamos otra distinta, podemos tener problemas.
- 2. Fijarse en el número de descargas de la app.** Si descargamos una aplicación de seguimiento masivo, no puede tener 100 descargas.
- 3. Permisos.** Si descargamos una aplicación sobre cómo perder barriga, no tiene sentido darle permisos sobre los SMS o llamadas.
- 4. No fiarse de títulos espectaculares** como: “Mira quien te rechazó en Facebook” o “Espía conversaciones de Whatsapp de otros usuarios”.
- 5. Sólo descargar aplicaciones de fuentes fiables,** y si es posible solo de tiendas oficiales.
- 6. No está de más bloquear los servicios “Premium” o de “tarificación especial” en nuestra línea de móvil.** Eso se lo debemos solicitar a nuestro operador de telefonía, he hecho ya hay alguno que no permite ese tipo de servicios.

Revisando los permisos de las apps

¿Aceptar o rechazar?

A continuación, te mostramos 5 aplicaciones muy distintas entre sí que acabas de descargar en tu dispositivo. Cada una de ellas tiene una descripción de sus funciones y una serie de permisos que quieren que aceptes.

Analiza los permisos con cuidado y determina aquellos que van acorde a la función de la app y debes o no aceptar. ¡Suerte!

COMENZAR



Códigos QR maliciosos

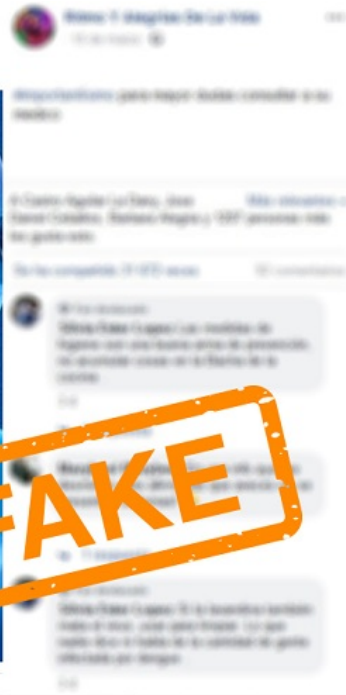


Evitemos más muertes

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.



FAKE



Bulos y *fake news*



Práctica (10')

- ▶ Localizar casos mediáticos en los que una *fake new* o bulo haya provocado desinformación entre los ciudadanos.

Ejemplos de *fake news*: COVID19

El coronavirus y los remedios falsos para prevenirlo: cómo la pseudociencia se aprovecha de situaciones de crisis

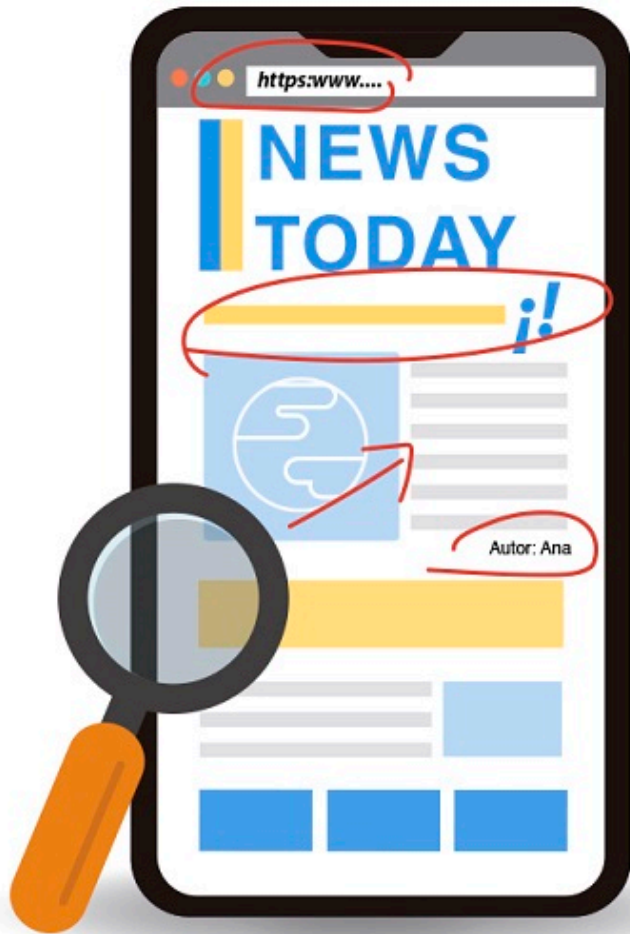


Las afirmaciones falsas de la imagen viral que quiere que no te pongas mascarilla



<https://maldita.es/malditobulo/2020/09/16/coronavirus-bulos-pandemia-prevenir-virus-covid-19/>

Cómo frenar la desinformación



¿Qué podemos hacer para detectarlos y prevenirlos?

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



Maldito Bulo

Newtral

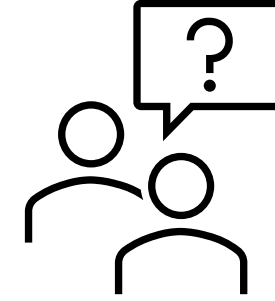
Snopes

Google Fact check tools



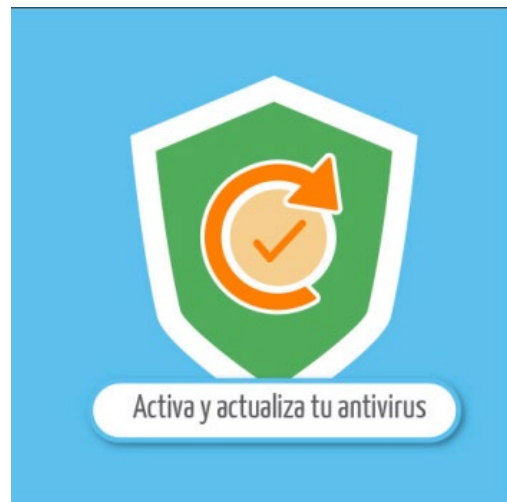
Medidas básicas de protección

¿Qué aspectos consideras que son esenciales?



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

Pon a punto tu dispositivo



Instala una herramienta antivirus



Actualiza el sistema operativo así como el resto de programas



Crea una cuenta de usuario diferente

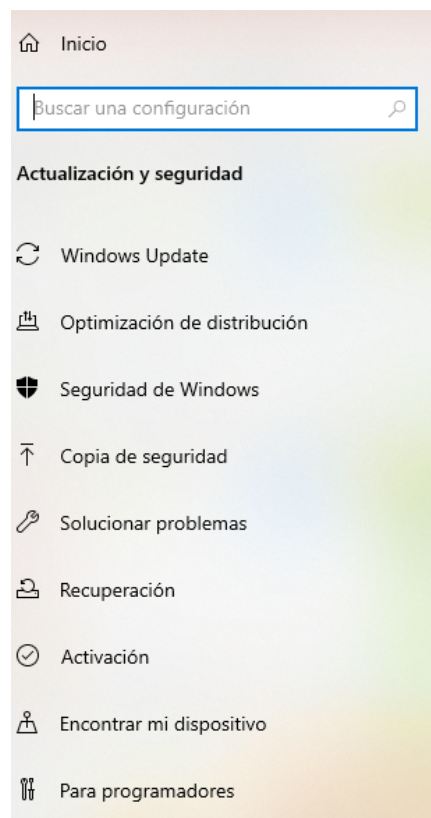
Actualizaciones automáticas

- ▶ Las actualizaciones son modificaciones realizadas sobre el sistema operativo o el software instalado en nuestros dispositivos. Su función es:
 - Mejorar aspectos de funcionalidad.
 - Mejorar la seguridad.
 - Corregir vulnerabilidades o errores.




Actualizaciones en Windows

- ✓ Iremos a Configuración > Actualización y Seguridad > Buscar actualizaciones.



Windows Update





 ¡Todo está actualizado!
Última comprobación: hoy, 3:19

Buscar actualizaciones

Actualización de características a Windows 10, versión 2004

La próxima versión de Windows está disponible con nuevas características y mejoras de seguridad. Cuando estés listo para la actualización, selecciona "Descargar e instalar".

[Descargar e instalar](#)

-  Pausar las actualizaciones durante 7 días
Ve a Opciones avanzadas para cambiar el período de pausa
-  Cambiar horas activas
Actualmente de 8:00 a 17:00
-  Ver historial de actualizaciones
Ver las actualizaciones instaladas en el dispositivo
-  Opciones avanzadas
Configuración y controles de actualización adicionales

Actualizaciones en MAC

- ▶ Actualizar el sistema operativo:
 - ✓ Iremos al logo de Apple > Preferencias del sistema > Actualizaciones del software.
- ▶ Actualizar las apps y software:
 - ✓ Descarga de la **página oficial** > Actualizaciones > **Mantener el Mac actualizado.**



Cuentas de usuario

- ▶ Si no gestionamos adecuadamente los roles y cuentas, corremos el riesgo de:



- ▶ Manipulación de información



- ▶ Acceso a nuestras cuentas



- ▶ Modificación de configuración

Por seguridad, lo ideal es mantener **un único usuario administrador por dispositivo** y **mantener al mínimo los privilegios del resto de cuentas de usuario** para evitar riesgos.

Cuentas de usuario en Windows

Existen diferentes tipos de cuentas:



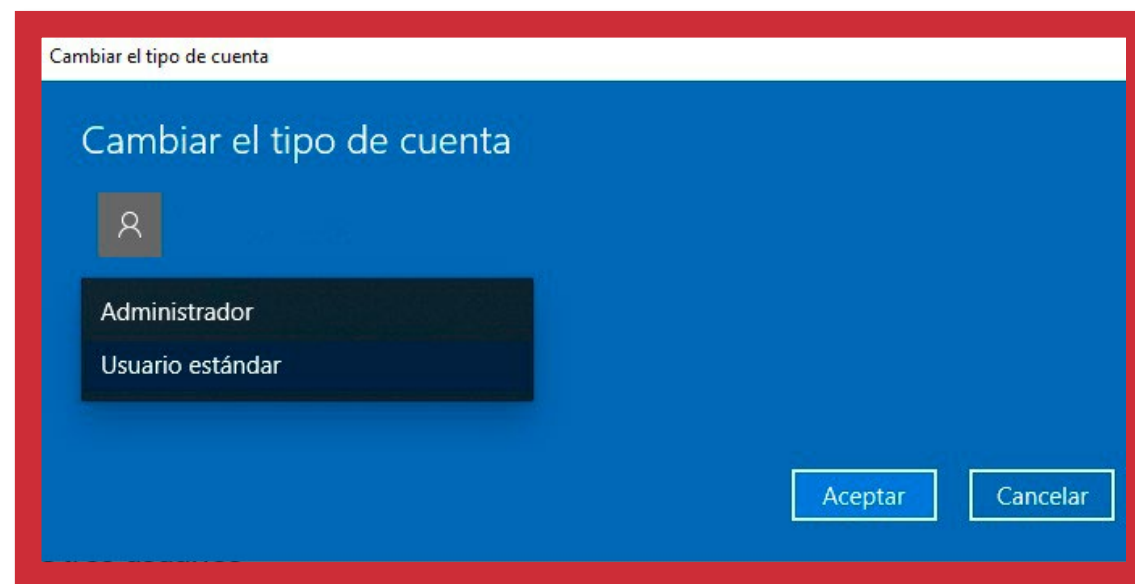
► Usuario Administrador



► Otros usuarios



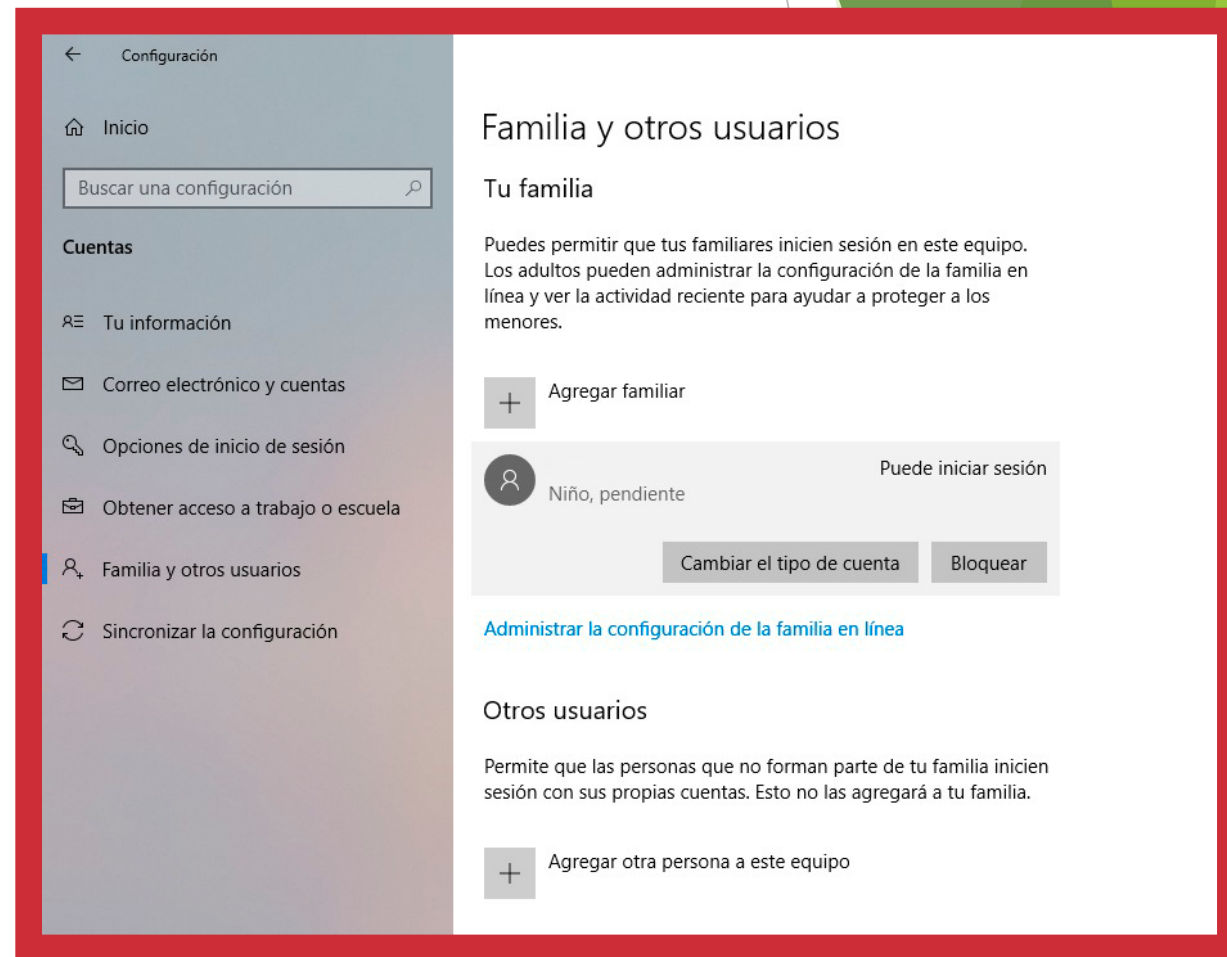
► Usuario "Tu familia"



Cuentas de usuario en Windows

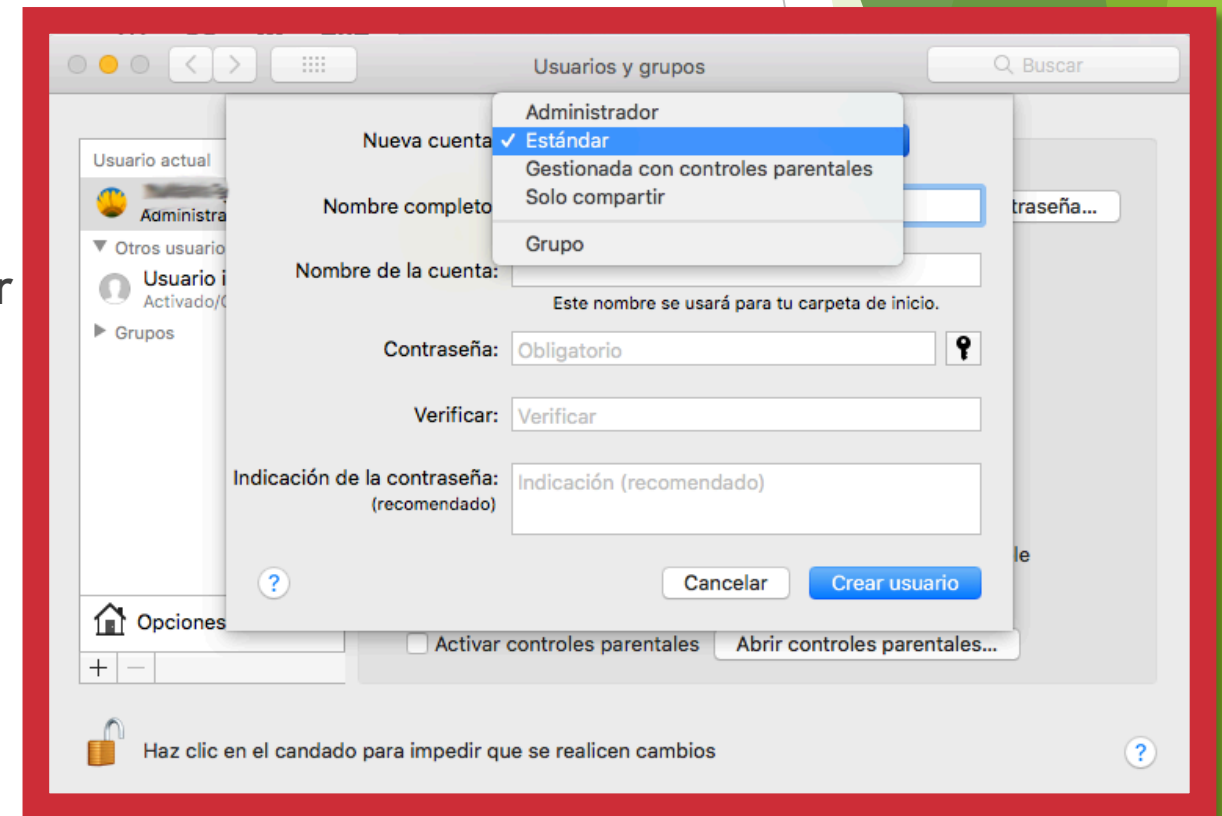
► Para crear cuentas:

- ❖ Iremos a la imagen de Windows en la parte inferior izquierda.
- ❖ Clic en **Configuración > Cuentas > Familia y otros usuarios** u **Otros usuarios**.



Cuentas de usuario en MAC

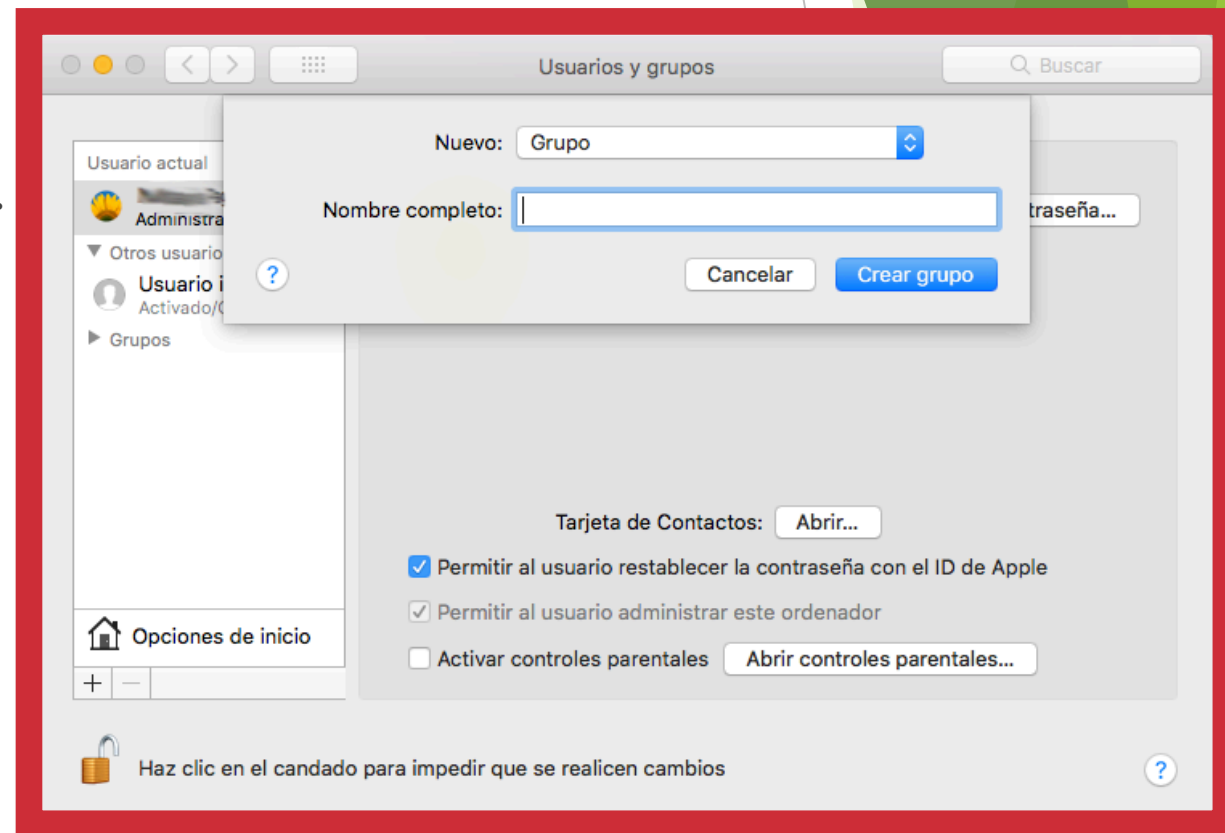
- ▶ Debemos tener en cuenta que esta configuración solo la puede realizar un administrador del sistema:
 - ❖ Logo Apple y clic en Preferencias del sistema > Usuarios y Grupos.
 - ❖ Luego, clic sobre el candado para que se desbloquee.
 - ❖ Ingresaremos con el nombre del administrador y contraseña de acceso.
 - ❖ Seleccionaremos en el menú Nueva carpeta y elegiremos el tipo de usuario que queremos crear.



Cuentas de usuario en MAC

► Otros perfiles y usuarios:

- ✓ **Crear Grupo:** permite que varios usuarios puedan tener acceso al dispositivo o a un archivo específico, sin el nivel administrativo.
- ✓ **Usuarios y grupos > clic en candado > Ingresamos con nuestros datos.**
- ✓ **Añadir > Nueva cuenta > Nuevo grupo > Crear grupo.**
- ✓ Luego, elegiremos los usuarios y podremos utilizar **Preferencias** para dar **permisos de compartir pantalla/archivos.**
- ✓ **Usuarios ocasionales:** No requieren contraseñas, ni tienen privilegios de ningún tipo. Son temporales.



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

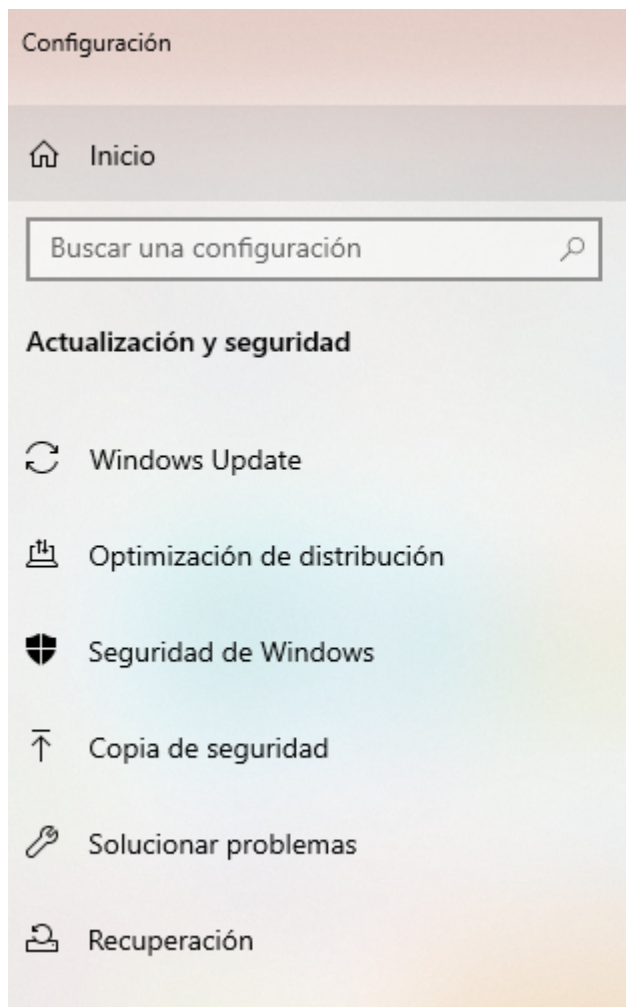
5 La proteges de ti mismo

DISCO EXTERNO (F:)

1,2 GB disponibles de 100 GB

¿ESTÁ SEGURO?
BORRAR TODO
ACEPTAR

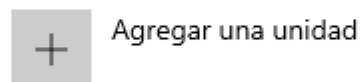
Copias de seguridad en Windows



Copia de seguridad

Copia de seguridad con Historial de archivos

Realiza una copia de seguridad de tus archivos en otra unidad y restáuralos si los originales se han perdido, están dañados o se han eliminado.



[Más opciones](#)

¿Buscas una copia de seguridad anterior?

Si creaste una copia de seguridad mediante la herramienta Copias de seguridad y restauración de Windows 7, todavía funcionará en Windows 10.

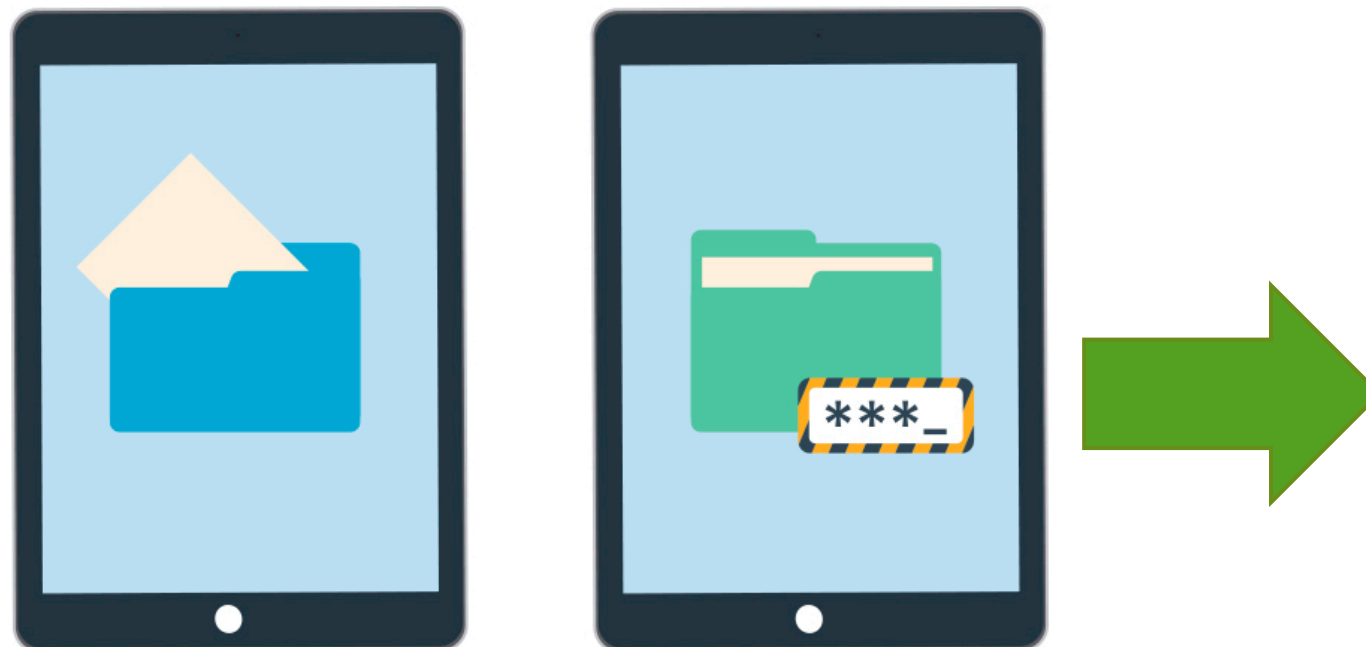
[Ir a Copias de seguridad y restauración \(Windows 7\)](#)

Copias de seguridad en Mac

- ▶ Time Machine: Permite realizar copias de seguridad de todos nuestros archivos de forma automática.



Cifra la información



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

- ▶ Utiliza alguna herramienta específica. Ej: VeraCrypt
- ▶ 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.

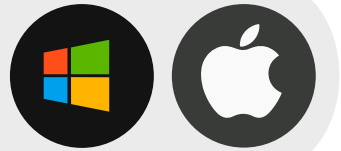
Configuración del router/AP (I)

- ▶ La seguridad de las redes inalámbricas de nuestros dispositivos es fundamental. A continuación, vamos a ver algunas medidas de seguridad a implementar en nuestro router:

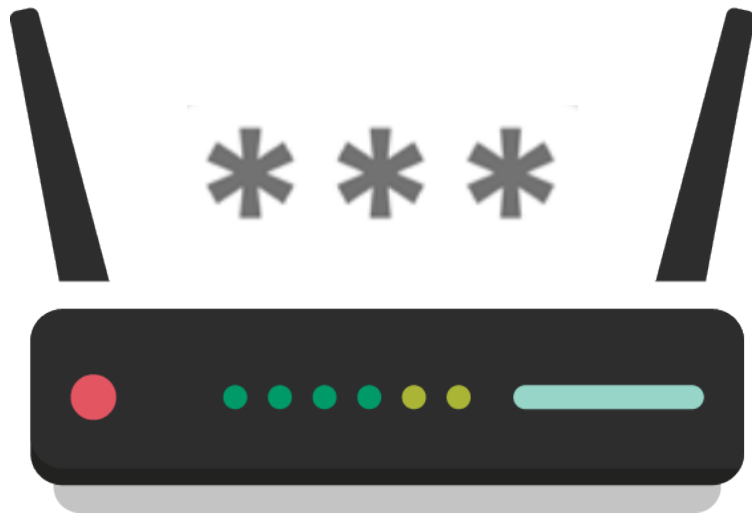


Modificar el SSID

Desactivar WPS



Configuración del router/AP (II)



Contraseñas de acceso y administración

Deshabilitar conexión remota

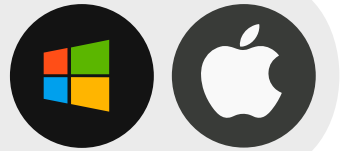


Configuración del router/AP (III)



Cifrado

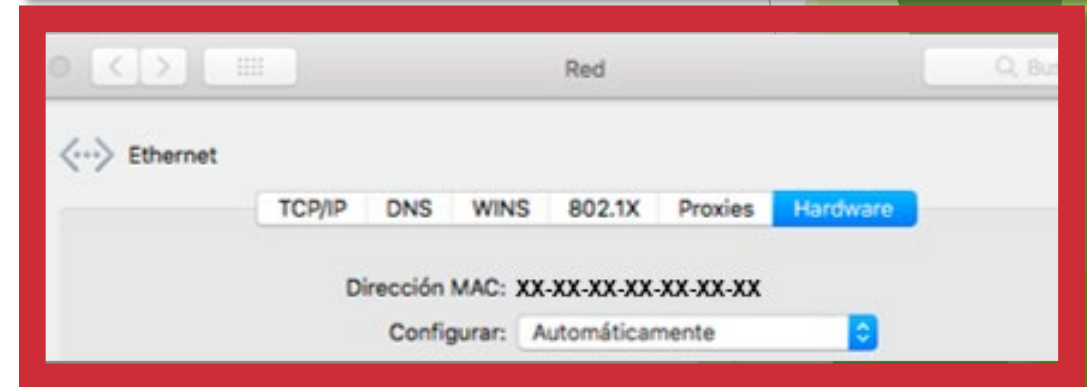
Limitar conexiones, ancho de banda y tiempo de conexión



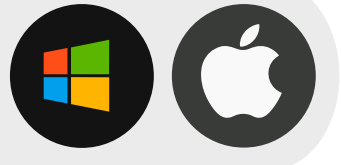
Configuración del router/AP (IV)

- ▶ Otra buena práctica que podemos seguir es revisar eventualmente los dispositivos que están conectados a nuestra red y realizar un filtrado por dirección MAC. Conociéndola, podemos crear una lista blanca de direcciones permitidas.
- ▶ Para conocer nuestra dirección en **Windows**:
 - MS-DOS > ipconfig/all.
- ▶ Para conocer nuestra dirección en **Mac**:
 - Preferencias del sistema > Redes > Avanzado > Ethernet/AirPort.

```
Adaptador de LAN inalámbrica Wi-Fi:  
  
Sufijo DNS específico para la conexión. . . :  
Descripción . . . . . :  
Dirección física. . . . . : XX-XX-XX-XX-XX-XX  
DHCP habilitado . . . . . :
```



Recuerda **visualizar todos los dispositivos conectados a la red cada cierto tiempo e identificar aquellos de confianza.**

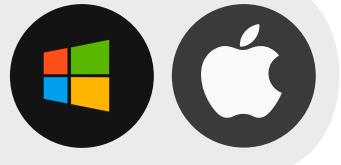


Configuración del router/AP (V)

- ▶ Crear una red de invitados no está disponible para todos los routers, pero permitirá compartir nuestra conexión en una red distinta a la principal.

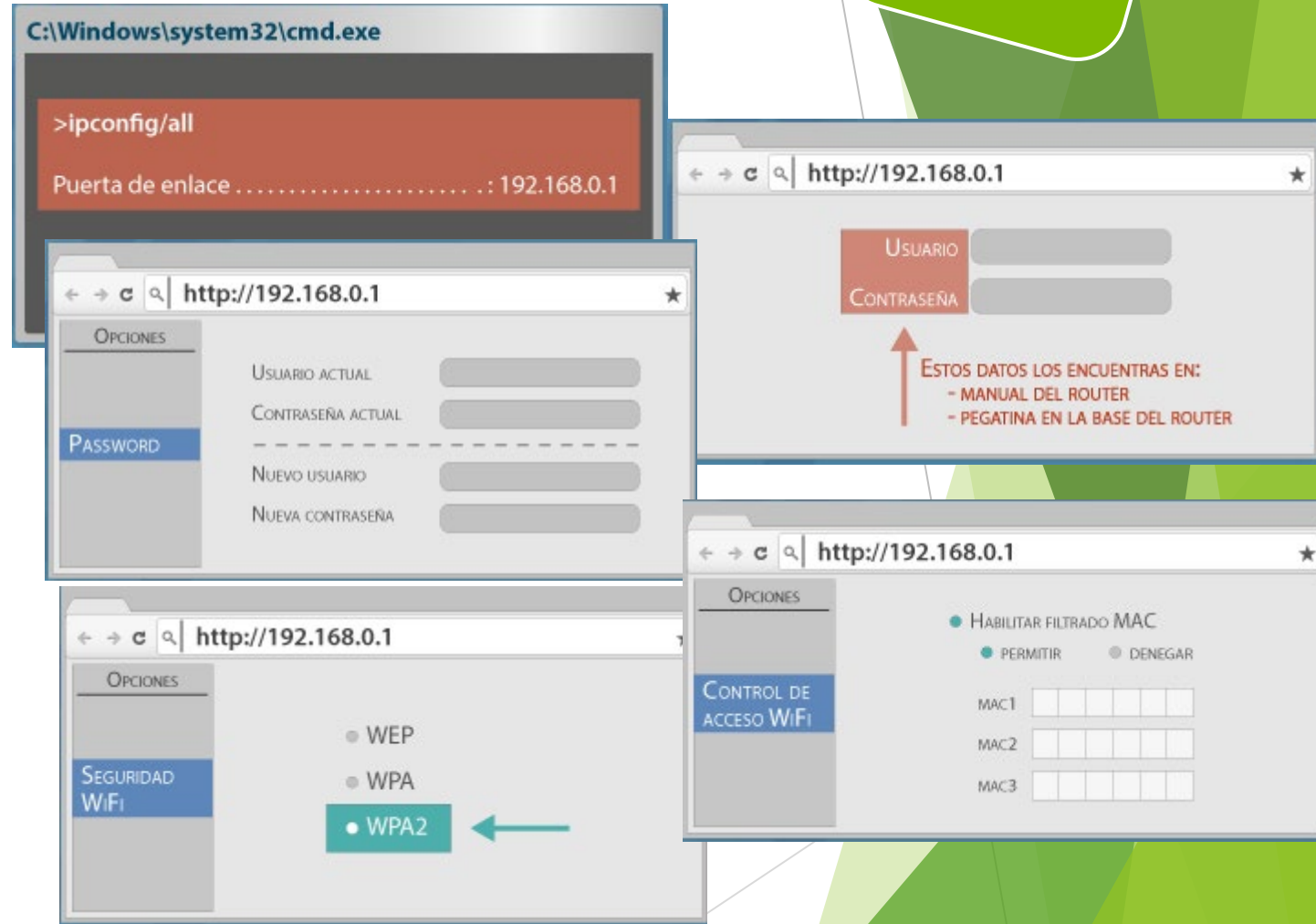


- Ve a los **Ajustes** del router mediante nuestra **dirección IP (192.168.1.1)**.
- Iremos a la **Configuración de las redes inalámbricas > Red para invitado**.
 - Nombre y contraseña.
 - Método de autenticación (WPA2).
 - Tipo de red (2,4 GHz).



Resumiendo:

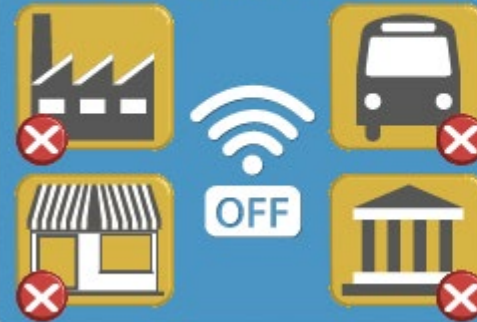
- ▶ Cambia la contraseña de acceso a la configuración del router.
- ▶ Actualiza la contraseña para conectarte a la red.
- ▶ Asignar el sistema de seguridad WPA2.
- ▶ Modifica el nombre de la wifi o SSID.
- ▶ Habilita el filtrado por MAC (o dirección física).



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.



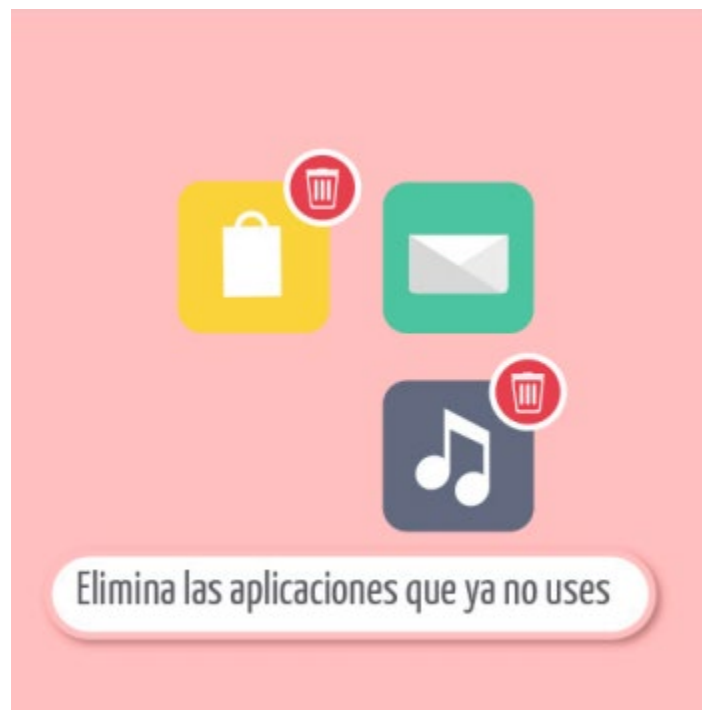
5. Sé precavido y mantén actualizados tus dispositivos y sus aplicaciones.



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



Y de manera adicional...



Buenas prácticas ciberseguras

Y si teletrabajas, que sea de manera cibersegura también

Seguridad en el marco docente

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.

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.

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.

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

incibe
INSTITUTO NACIONAL DE CIBERSEGURIDAD
@INCIBE | INCIBE | @INCIBE

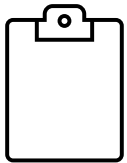
017

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

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

Práctica (5')



- ▶ **Cómo enseñarías a un alumno a gestionar de manera segura sus contraseñas. Elabora un listado a modo decálogo con las mejores ideas que se te ocurran.**

Cómo gestionar de manera segura las contraseñas (I): contraseñas robustas

 **Contraseñas complejas** ✓

Utilizar más de 8 caracteres incluyendo mayúsculas, minúsculas, números y caracteres especiales.

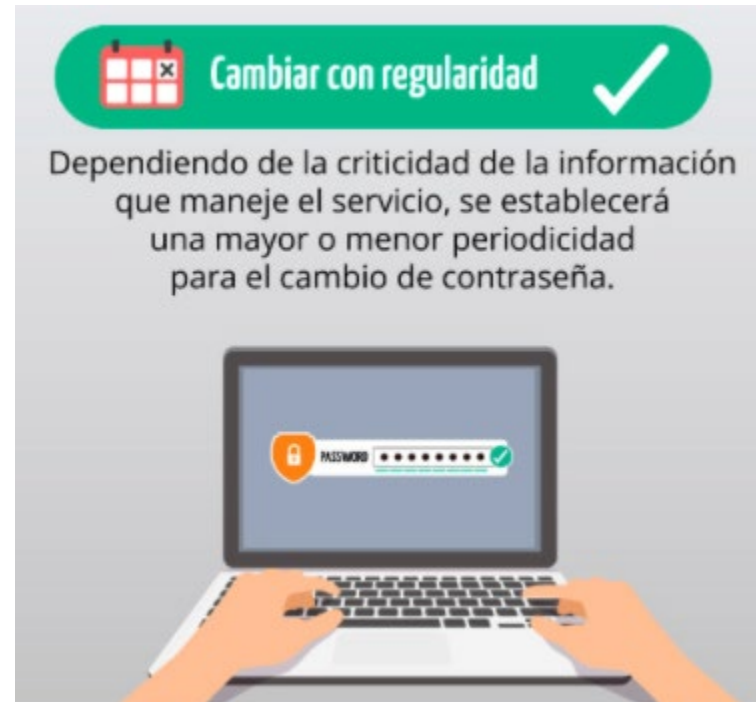
  **Contraseñas diferentes** ✓

No reutilizar contraseñas, usa contraseñas diferentes para distintos servicios.

Ranking contraseñas más vulnerables

1. PASSWORD 123456 ✗
2. PASSWORD password ✗
3. PASSWORD 123456789 ✗
4. PASSWORD 12345678 ✗
5. PASSWORD 12345 ✗

Cómo gestionar de manera segura las contraseñas (II): cambiarla frecuentemente



Cómo gestionar de manera segura las contraseñas (III): reglas nemotécnicas

Clave simple

Perro26



Clave Robusta

7377626

Clave simple

Perro26!



Cambiamos algunas letras por números
P3rr026!



Jugamos con las mayúsculas para no crear patrones
P3rR026!

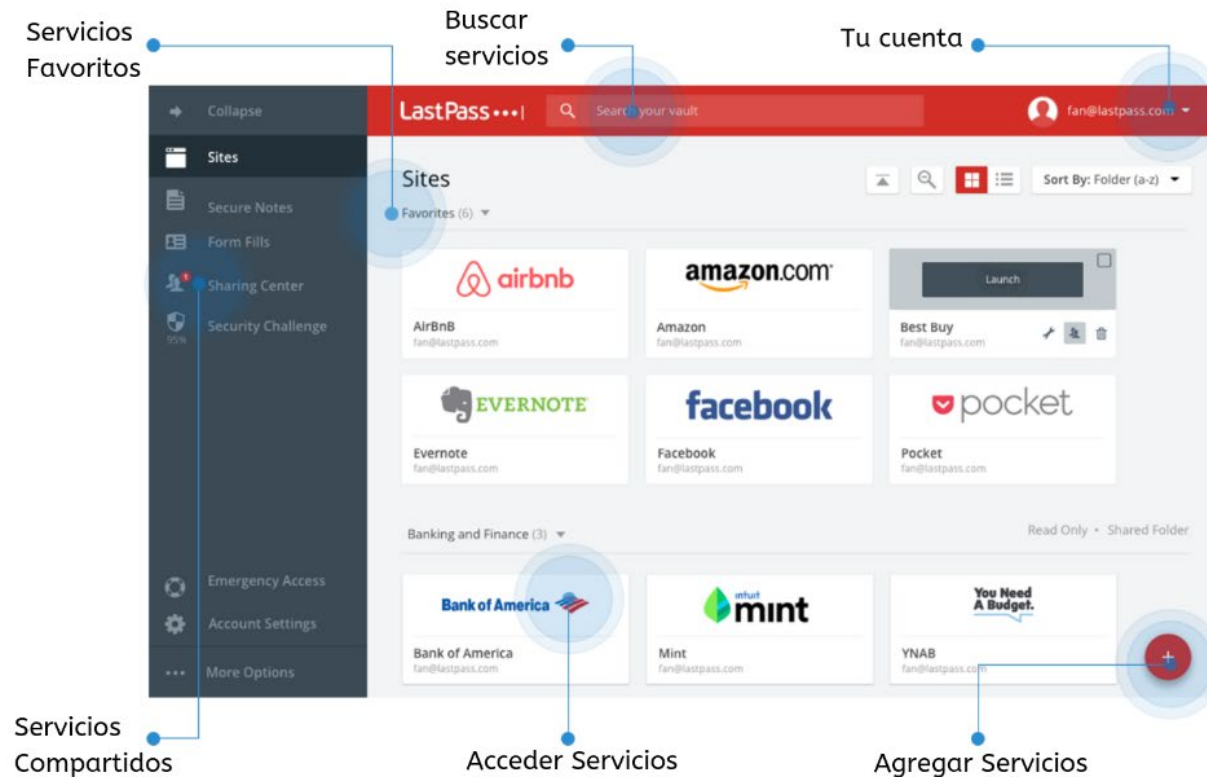


Por último, de igual modo movemos los números del final para romper el patrón
2P3rR06!

Clave robusta

2P3rR06!

Cómo gestionar de manera segura las contraseñas (IV): gestores de contraseñas



Cómo gestionar de manera segura las contraseñas (V): doble verificación



Smartphones y tablets: protégelos

1 Vincula tu dispositivo móvil a una [cuenta Google](#) en tu móvil Android.

2 Utiliza una clave de bloqueo para tu dispositivo. Si no es biométrica, recuerda usar una [contraseña robusta](#).

3 Activa el sistema de [actualizaciones automáticas](#) de tu dispositivo y aplicaciones, pues con esto se corrigen los defectos en seguridad que puedan tener.

4 Usa [aplicaciones de seguridad](#) que añadan una capa extra de seguridad a tu dispositivo, como por ejemplo un antivirus.

5 Protege tu información mediante [copias de seguridad](#). De este modo tendrás una copia de respaldo en caso de pérdida o borrado de tu dispositivo.



6 Desactiva las conexiones inalámbricas una vez hayas terminado de usarlas (wifi, Bluetooth, NFC).

7 Cuando instales aplicaciones, [revisa siempre quién es el desarrollador así como las opiniones y valoraciones del resto de usuarios](#). ¡Y acuérdate de [eliminar las que ya no uses](#)!



8 [Otorga los permisos a las apps que sean imprescindibles](#) para su correcto funcionamiento y revisa siempre que sean coherentes con la funcionalidad de la app.



9 [Evita prácticas de riesgo](#) con el rooting en Android.



10 Si vas a deshacerte de tu móvil, [asegúrate de borrar toda la información](#) que contiene para no dejar rastro.



11 Apóyate en [herramientas de control parental](#) si el dispositivo lo va a utilizar un menor.



Smartphones y tablets: protégelos

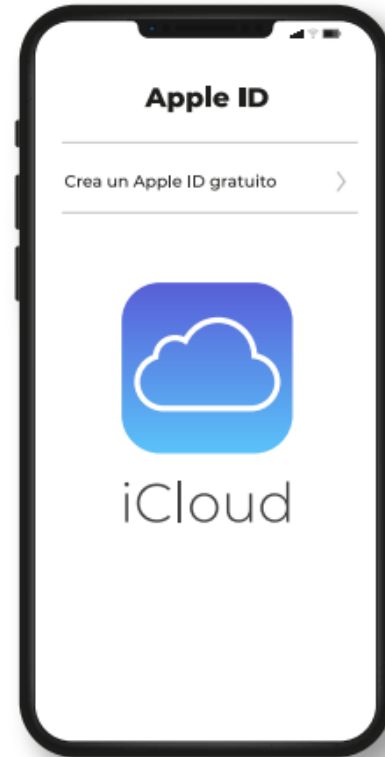
1 Vincula tu dispositivo móvil a una cuenta de [iCloud](#)

2 Utiliza una clave de bloqueo para tu dispositivo. Si no es biométrica, recuerda usar una [contraseña robusta](#).

3 Activa el sistema de [actualizaciones automáticas](#) de tu dispositivo y aplicaciones, pues con esto se corrigen los defectos en seguridad que puedan tener.

4 Usa [aplicaciones de seguridad](#) que añadan una capa extra de seguridad a tu dispositivo, como por ejemplo un antivirus.

5 Protege tu información mediante [copias de seguridad](#). De este modo tendrás una copia de respaldo en caso de pérdida o borrado de tu dispositivo.



6 Desactiva las conexiones inalámbricas una vez hayas terminado de usarlas (wifi, Bluetooth, NFC).

7 Cuando instales aplicaciones, [revisa siempre quién es el desarrollador así como las opiniones y valoraciones del resto de usuarios](#). ¡Y acuérdate de [eliminar las que ya no uses!](#)



8 [Otorga los permisos a las apps que sean imprescindibles](#) para su correcto funcionamiento y revisa siempre que sean coherentes con la funcionalidad de la app.



9 [Evita prácticas de riesgo](#) con el [jailbraiking](#) en iOS.



10 Si vas a deshacerte de tu móvil, [asegúrate de borrar toda la información](#) que contiene para no dejar rastro.



11 Apóyate en [herramientas de control parental](#) si el dispositivo lo va a utilizar un menor.



Smartphones y tablets: protégelos



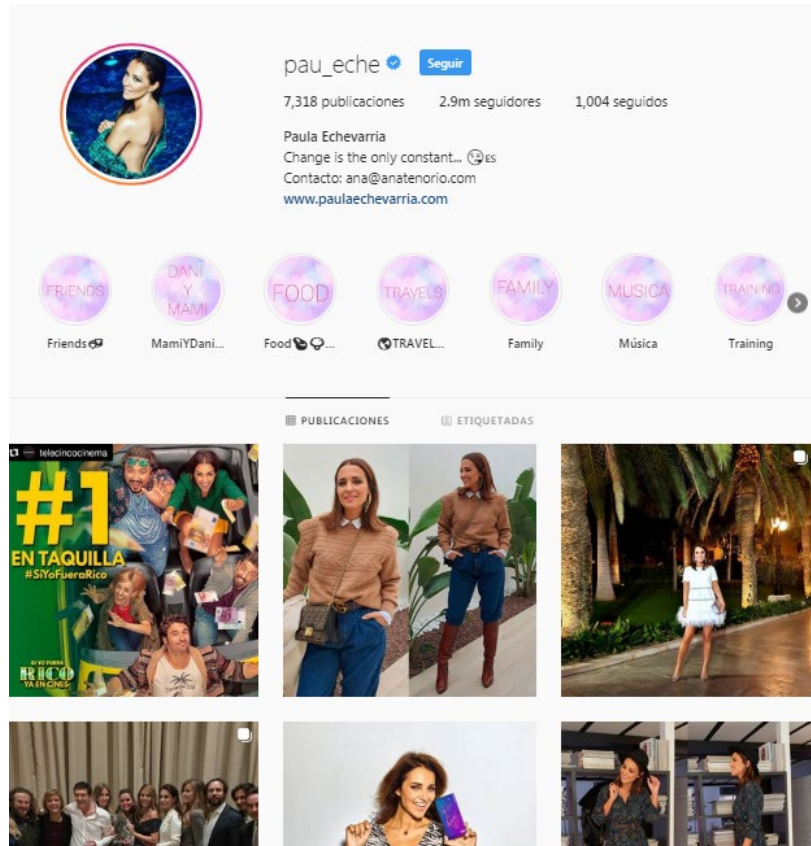
Privacidad, identidad y reputación online

¿Sabes qué es la identidad digital?

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

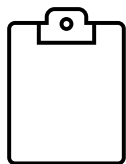


¿Qué pasa con tu privacidad online?



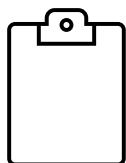
¿Cuánta
información
existe sobre ti en
Internet?

Práctica (5')

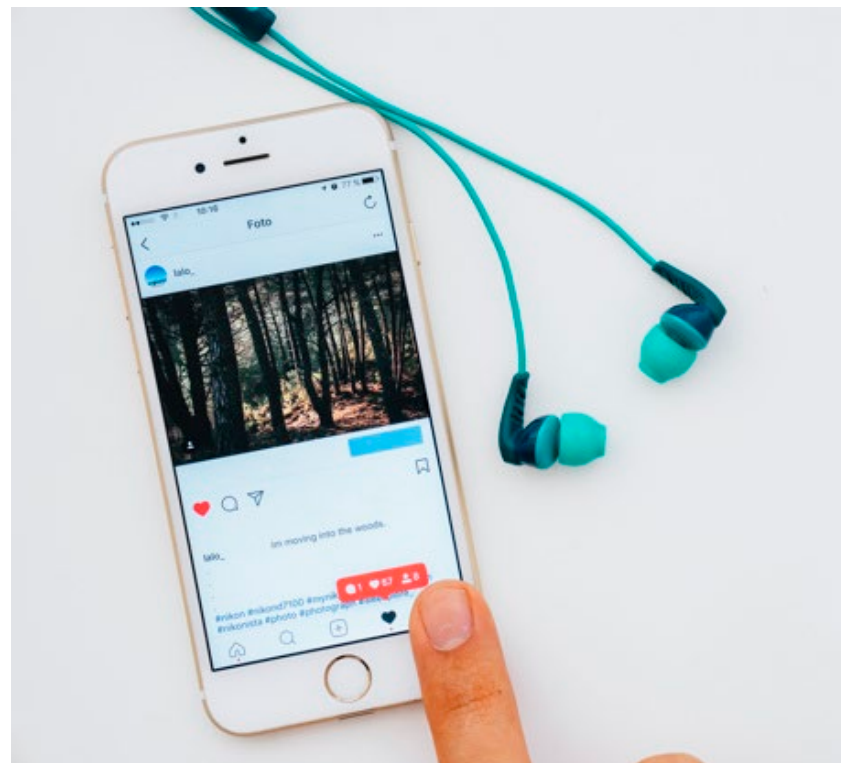


- ▶ **Egosurfing.** Realiza una búsqueda en distintos motores de búsqueda únicamente introduciendo tu nombre.

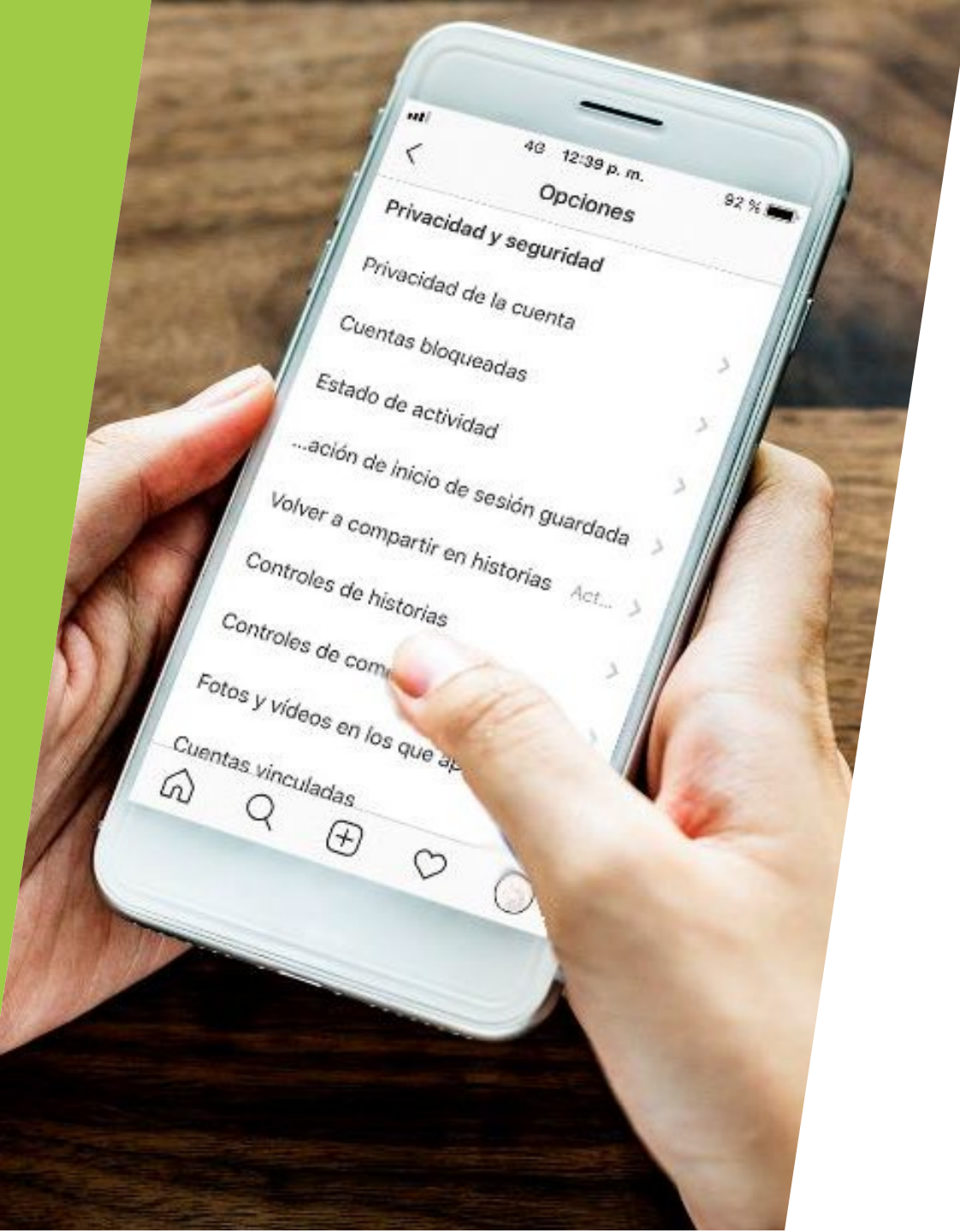
Práctica (5')



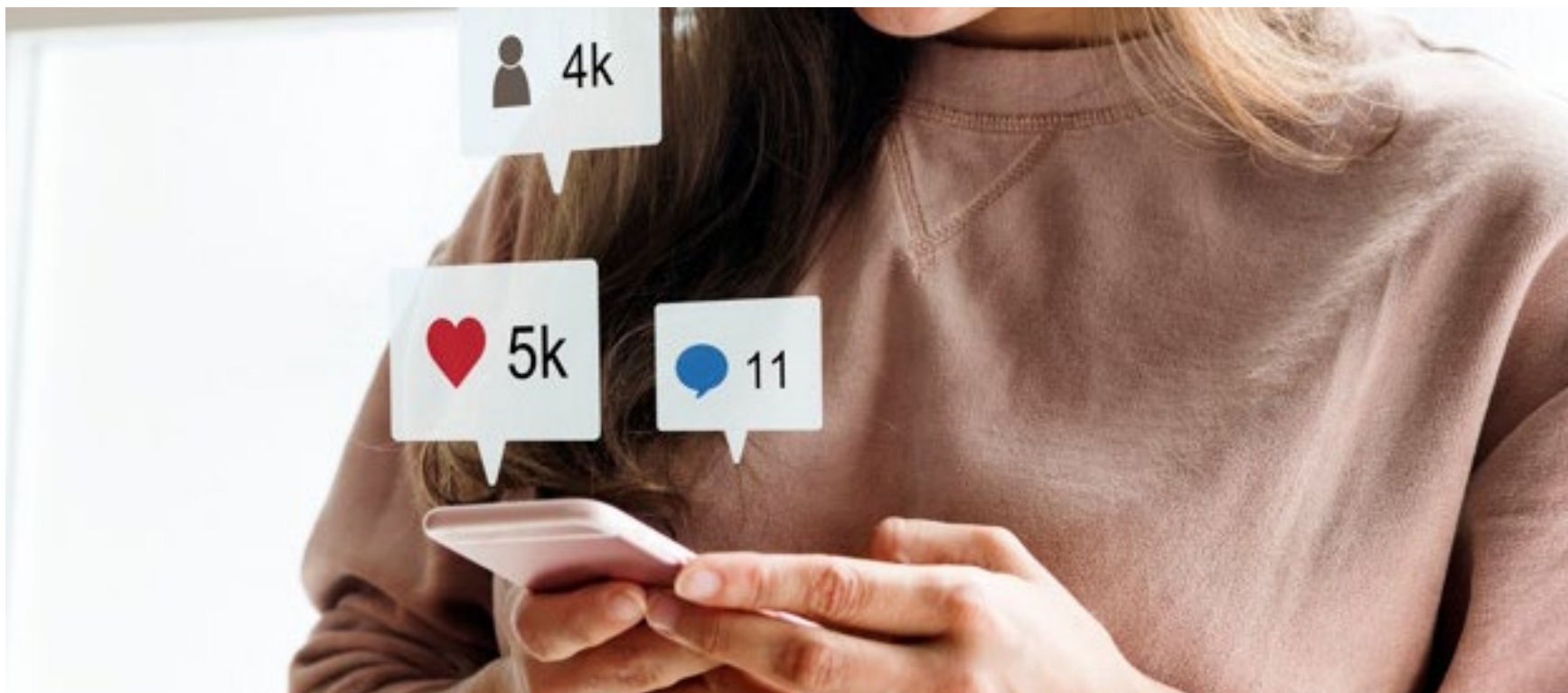
- ▶ Automatizando la búsqueda de información con herramientas OSINT (Lampyre & theHarvester)



¿Tienes una identidad digital positiva?



¿Configuras
adecuadamente
tus perfiles?

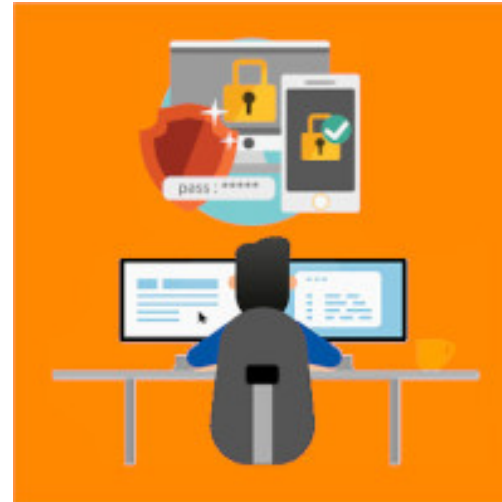


¿Quiénes son tus contactos online?



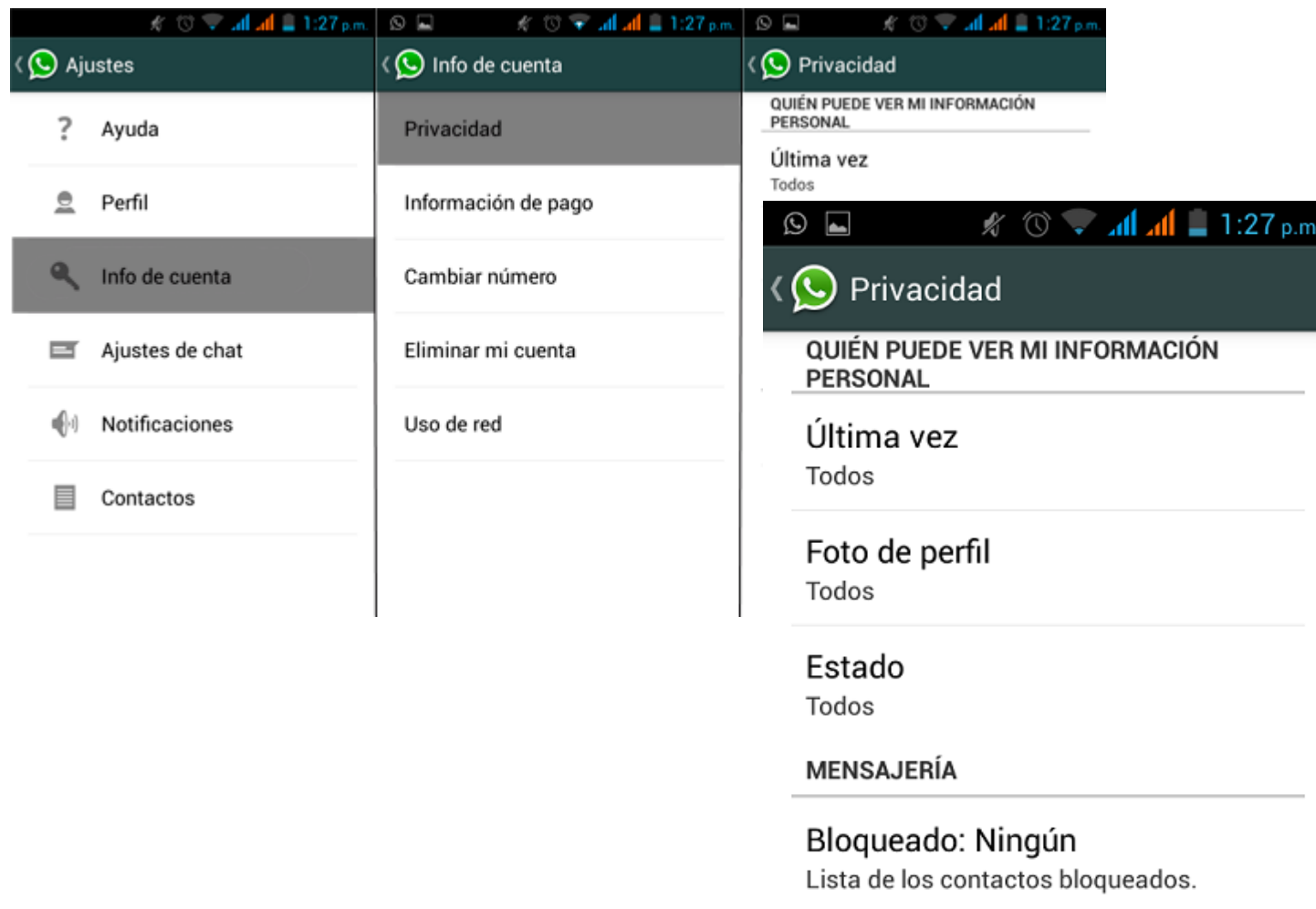
¿Conoces los
riesgos asociados
al sexting?

Configuraciones de privacidad útiles



Whatsapp

Seguridad en el marco docente



Centro de seguridad de Google

Seguridad en el marco docente

Google Centro de seguridad

Información general

En nuestros productos

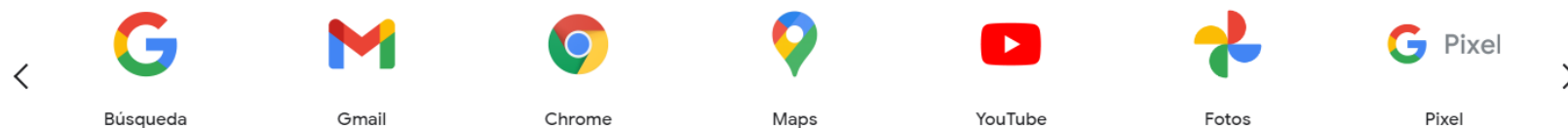
Seguridad y privacidad

Seguridad familiar

Equipo directivo

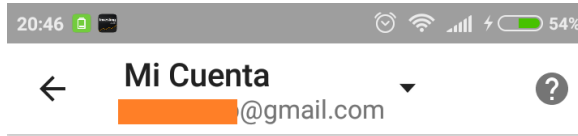
Cuenta de Google

La forma más segura de buscar.



<https://safety.google/>





Manuel
[redacted]@gmail.com
[ACTUALIZAR FOTO](#)



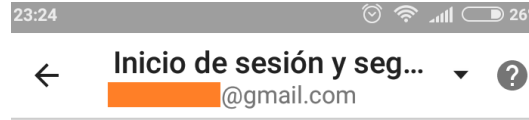
Inicio de sesión y seguridad
Controla tu contraseña y el acceso a tu cuenta de Google



Información personal y privacidad
Administra los ajustes de visibilidad y los datos utilizados para la personalización



Preferencias
Define tu idioma y el almacenamiento



Revisión de seguridad
Protege tu cuenta realizando una comprobación rápida de tus ajustes de seguridad y tu actividad
[EMPEZAR](#)

Inicio de sesión en Google

Contraseña
Cambiar tu contraseña

Verificación en dos pasos
Activada desde: 16 dic. 2017

Contraseñas de aplicación
Ninguna

«Ajustes > Cuentas > Google. También desde Ajustes de Google»



Revisión de seguridad

No se han detectado problemas

- ✓ **Tus dispositivos**
3 dispositivos usados recientemente
- ✓ **Actividad de seguridad reciente**
No ha habido eventos en estos 28 días
- ✓ **Verificación en dos pasos**
La verificación en dos pasos está activada

o riesgo a

Teléfono de recuperación

Google

23:24
← **Revisión de privacidad**
[redacted]@gmail.c



Te damos la bienvenida

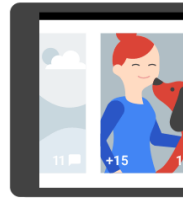
Elige la configuración de privacidad para ti

Revisa y ajusta qué datos utilizamos para personalizar tu experiencia y qué información compartes con otros

EMPEZAR AHORA

1. Administrar la configuración de Google Fotos

Elige si quieres quitar la información de tus fotos cuando las compartes



Quitar la ubicación geográfica de los elementos compartidos por un enlace

Afecta a los elementos compartidos por enlace, pero no por otros métodos

SIGUIENTE

1. Administrar la configuración de Google+

2. Elegir qué información Google+ compartes con los demás

Decide quién puede ver tu información y qué información quieres publicar o mantener privada. [Más información](#)



Muestra estas pestañas de perfil

3. Personalizar tu experiencia de Google

Desde mejores opciones para desactivar hasta resultados más rápidos en herramientas y los servicios de Google, más rápidos y útiles con los datos que nos permites guardar en tu cuenta, tú puedes ver tu actividad.



Actualmente, estos controles no están disponibles

Historial de ubicaciones

Historial de búsquedas de YouTube



Actualmente, estos controles no están disponibles

Actividad en la Web y en Aplicaciones

Historial de ubicaciones

Información de los dispositivos

Actividad de Voz y Audio

Historial de búsquedas de YouTube

Historial de reproducciones de YouTube

Historial de búsquedas de YouTube

SIGUIENTE

Seguridad en el marco docente



Tu configuración de privacidad ya está actualizada

Eres responsable de controlar siempre tus datos y tu información. Puedes volver aquí para ajustar la configuración de privacidad en cualquier momento.

- ✓ 1. Se ha revisado la configuración de Google Fotos
- ✓ 2. Se ha revisado la configuración de Google+
- ✓ 3. Controles de la actividad de tu cuenta revisados
- ✓ 4. Se ha revisado la configuración de anuncios

«Ajustes > Cuentas > Google. También desde Ajustes de Google»



Navegadores

Borrar datos de navegación

Básico Configuración avanzada

Intervalo de tiempo Desde siempre

- Historial de navegación
4.642 elementos
- Historial de descargas
1.030 elementos
- Cookies y otros datos de sitios
De 125 sitios web
- Archivos e imágenes almacenados en caché
228 MB
- Contraseñas y otros datos de inicio de sesión
No hay
- Datos de Autocompletar formulario

Cancelar Borrar datos

Borrar datos de navegación



Navegadores



Has iniciado una sesión de incógnito

Ahora puedes navegar de forma privada; las otras personas que usen este dispositivo no verán tu actividad. No obstante, se guardarán las descargas y los marcadores. [Más información](#)

Chrome no guardará la siguiente información:


- Tu historial de navegación
- Las cookies y los datos de sitios web
- La información introducida en formularios

Es posible que tu actividad todavía sea visible para:

- Los sitios web que visites
- Tu empresa o centro educativo
- Tu proveedor de servicios de Internet

Navegar por Internet sin que se almacenen los datos de búsqueda, historial, caché, etc.

Navegadores que no invaden privacidad Seguridad en el marco docente



Privacy, simplified.

Seamlessly take control of your personal information, no matter where the Internet takes you.



Enter what you want to calculate or know about:

Web Apps Examples Random



Yippy search results for "Oficina de Seguridad del Internauta".

Did you mean [Oficina de Seguridad del "inter nauta"?](#)

- [Oficina de Seguridad del Internauta](#) new window preview
Herramientas de seguridad gratuitas. ... © OSI - Oficina de Seguridad del Internauta. Poste al día. Avisos de seguridad, Blog, Historias Reales ¿Cuánto sabes? [https://www.osi.es](#) - - Yippy Index V
- [Oficina de Seguridad del Internauta - Incibe | Facebook](#) new window preview
Ya os hemos contado en varias ocasiones y muchos de vosotros conocéis las medidas de seguridad que debe tener una tienda. ... Oficina de Seguridad del Internauta... [https://www.facebook.com/osiseguridad](#) - - Yippy Index V
- [Oficina de Seguridad del Internauta - Google+](#) new window preview
Oficina de Seguridad del Internauta's posts. Post has attachment. Oficina de Seguridad del Internauta. Public... [https://plus.google.com/100714825184222635522](#) - - Yippy Index V
- [Oficina De Seguridad Del Internauta, Os!es, os!es, www...](#) new window preview
... oficina de seguridad del Internauta Cheapest car insurance rate. Car insurance is obligatory for each owner of the vehicle. It covers the risk of damage that you... [https://www.ivantils.com/www/os!es](#) - - Yippy Index V
- [La oficina de Seguridad del Internauta - desarrolloweb.com](#) new window preview
... La oficina de Seguridad del Internauta pone a disposición de forma gratuita una importante colección de recursos, recomendaciones, herramientas, ... [www.desarrolloweb.com/...cna-seguridad-internauta-2207.html](#) - - Yippy Index V
- [Oficina De Seguridad Del Internauta, Os!es, wwwos!es...](#) new window preview
Oficina De Seguridad Del Internauta, Os!es, wwwos!es, os!es. Last update: 471 days ago [https://www.nufido.com/www/os!es](#) - - Yippy Index V



Startpage search results for "oficina de seguridad del internauta".

Web Imágenes Vídeos Avanzada Marque esta búsqueda

[Oficina de Seguridad del Internauta | https://www.osi.es/](#) Proxy Destacar
Un servicio del Gobierno de España para proporcionar información y soporte sobre los problemas de seguridad que surgen al navegar por Internet.

[Herramientas | Oficina de Seguridad del Internauta https://www.osi.es/es/herramientas](#) Proxy Destacar
Ponemos a tu disposición una serie de herramientas gratuitas que te ayudarán ...

[¿Quiénes somos? | Oficina de Seguridad del Internauta https://www.osi.es/es/quienes-somos](#) Proxy Destacar
En la Oficina de Seguridad del Internauta (OSI) de INCIBE proporcionamos la ...


[Desinfecta tu ordenador | Oficina de Seguridad del Internauta https://www.osi.es/es/desinfecta-tu-ordenador](#) Proxy Destacar
Tu ordenador tiene virus y no sabes cómo eliminarlos? ¡Estás en el sitio ...

[Oficina de Seguridad del Internauta recursostic.educacion.es/heda/web/familias-conectads/n...](#) Proxy Destacar
La "Oficina de Seguridad del Internauta" (OSI) es un servicio del Gobierno para




Aplicaciones de bloqueo de publicidad

Seguridad en el marco docente



Aplicación Adblock Browser

Del equipo que está detrás de Adblock Plus, el bloqueador de anuncios para navegadores de escritorio más popular del mundo, Adblock Browser está ahora disponible para dispositivos iOS y Android.

Consíguelo en el **App Store**  **DISPONIBLE EN Google Play**

Anuncios en la lista negra

Una lista de filtros que bloquea anuncios (por ejemplo, EasyList) según los ajustes de idioma de tu navegador.

Anuncios Aceptables

Una función que ayuda a una mejor web permitiendo anuncios no intrusivos y respetuosos que cumplen con los criterios de Anuncios Aceptables acordados por el Comité de Anuncios Aceptables.



Brainstorming (5')

- ▶ ¿Qué otras medidas/configuraciones se os ocurren para proteger la privacidad de los usuarios?

We Are
here to
—help—



Oficina de Seguridad del Internauta

Seguridad en el marco docente



Oficina de Seguridad del Internauta

Seguridad en el marco docente



Información y actualidad

Campañas de concienciación temáticas



#OSlavis

Avisos de seguridad



Los ciberdelincuentes, ¿quiénes son?



Dispositivos móviles



IoT, los riesgos de un mundo hiperconectado



Redes Sociales



Blog
Historias reales



¡Contraseñas seguras!



Oficina de Seguridad del Internauta

Seguridad en el marco docente



Servicios de soporte



OSI Oficina de Seguridad del Internauta
Servicio ANTIBOTNET

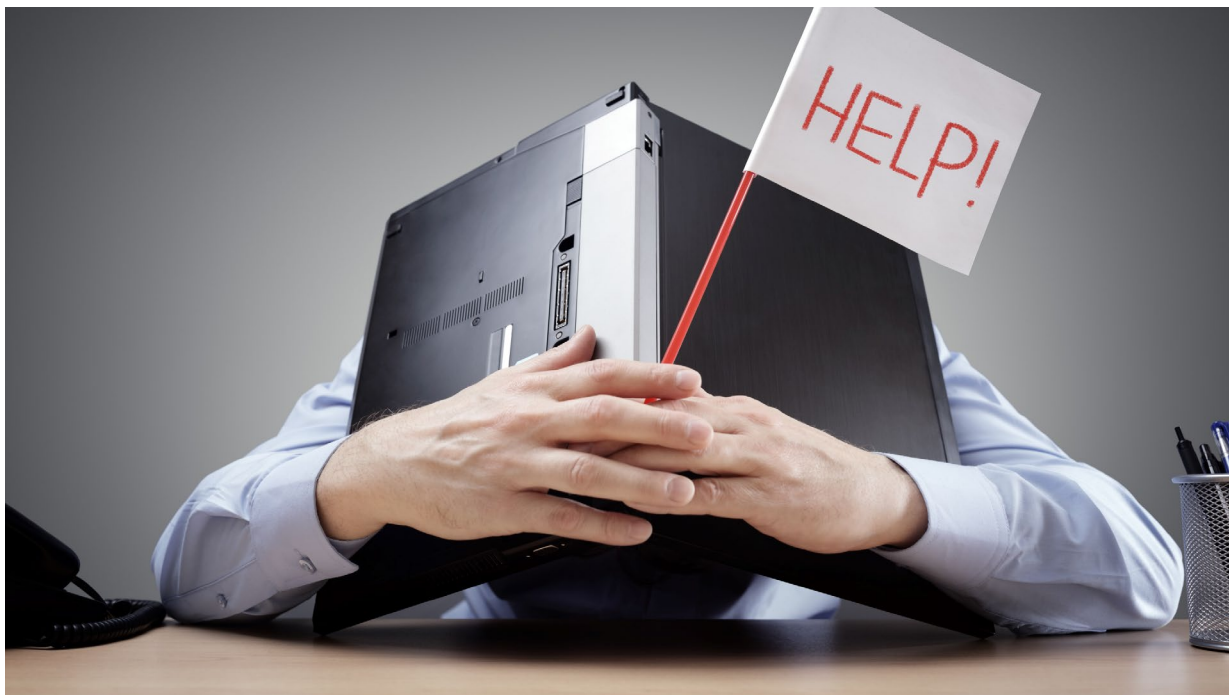


Guías, videotutoriales para configurar la **PRIVACIDAD** y **SEGURIDAD**:



Conan mobile





¿Sigues necesitando ayuda?

Línea de Ayuda en Ciberseguridad

Seguridad en el marco docente

TU AYUDA EN
CIBERSEGURIDAD



[WhatsApp: 900 116 117](https://www.whatsapp.com/message/900116117)

[Telegram: @INCIBE017](https://www.telegram.com/@INCIBE017)

 www.incibe.es

 contacto@incibe.es

    [@incibe](https://www.facebook.com/incibe)



Gracias por tu atención

<https://www.linkedin.com/in/ruthgarciaruiz/>

