

JORNADAS FORMATIVAS

# Cuestiones claves sobre ciberseguridad



**¿Sabes protegerte ante un ciberataque?**

**¿Sabes cómo actuar si has sido víctima de un ciberataque?**

# Actualidad y tendencia

20/04/2022 – El Comercio

Un ciberataque paraliza el sistema informático del Ayuntamiento de Gijón e interrumpe servicios ciudadanos.

20/06/2022 – El Español

¿Eres cliente del BBVA? Cuidado con este virus que puede robar las claves de acceso a tu cuenta.

10/02/2022 – El País

Nueve de cada diez empresas españolas sufrió al menos un ciberataque en 2021.

(\*) <https://www.incibe.es/sala-prensa/notas-prensa/incibe-gestiona-mas-100000-incidentes-ciberseguridad-durante-2021>

12/05/2022 (\*)

**INCIBE (Instituto Nacional de Ciberseguridad) gestiona más de 100.000 incidentes de ciberseguridad durante 2021.**



90.168 corresponden a ciudadanos y a empresas y 680 a operadores estratégicos, según el Balance de Ciberseguridad 2021.

29/06/2022 – El Español

Detenido en Málaga por espiar a una compañera al instalar un software de control remoto en el móvil.

# ¿Cómo puede afectarnos?



# Objetivo de los ataques

**Personas**



**Concienciación y formación**

**Sistemas**



**Actualización y configuración**

**Ambos**

# Personas: Concienciación y formación

24/05/2022 – RTVE

## El Foro económico de Davos apuesta por fortalecer al individuo ante el aumento de ciberataques

Los participantes en la sesión de tecnología e innovación de la cita en Suiza han puesto el foco en la enseñanza al individuo para blindar tanto la seguridad del sistema como la de las personas que lo componen.



"The major risk is not so much I.T. security in terms of technical issues, it's human failure."

Jürgen Stock, the Interpol secretary-general, joins @CNBCKaren's Davos panel on the risks we face on cybersecurity. #WEF22

08/05/2022 – EITB MEDIA

## Según los expertos, nadie está 100 % preparado para hacer frente a un ciberataque

El año pasado, la Ertzaintza gestionó casi 1.400 incidencias de este tipo; el 42% de ellas, buscan el fraude. Se estima que para cuando este año 2022 termine, los ciberataques habrán subido entre un 15 % y un 20%.

# Contraseñas

## ***Fuerza bruta***

Consiste en adivinar nuestra contraseña a base de ensayo y error, usando combinaciones con la información que conocen de nosotros, palabras y números al azar, etc. Generalmente lo ejecutan quienes nos conocen o tienen acceso a nuestra información personal nuestra.



## ***Por diccionario***

Utilizan un software que, de forma automática, trata de averiguar nuestra contraseña e intenta repetidamente acceder a nuestras cuentas hasta que lo consigue. Para esto además utilizan bancos de contraseñas.



## Contraseñas Fuertes

- Mínimo 10 caracteres.
- Combinación de mayúsculas, minúsculas, números y símbolos.

¿Es segura?

José.Pérez.García.11031980

Por qué hacerlo?

¡Recuerda!

Es importante cambiarlas cada cierto tiempo

**TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022**

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS [Learn about our methodology at hivesystems.io/password](https://hivesystems.io/password)

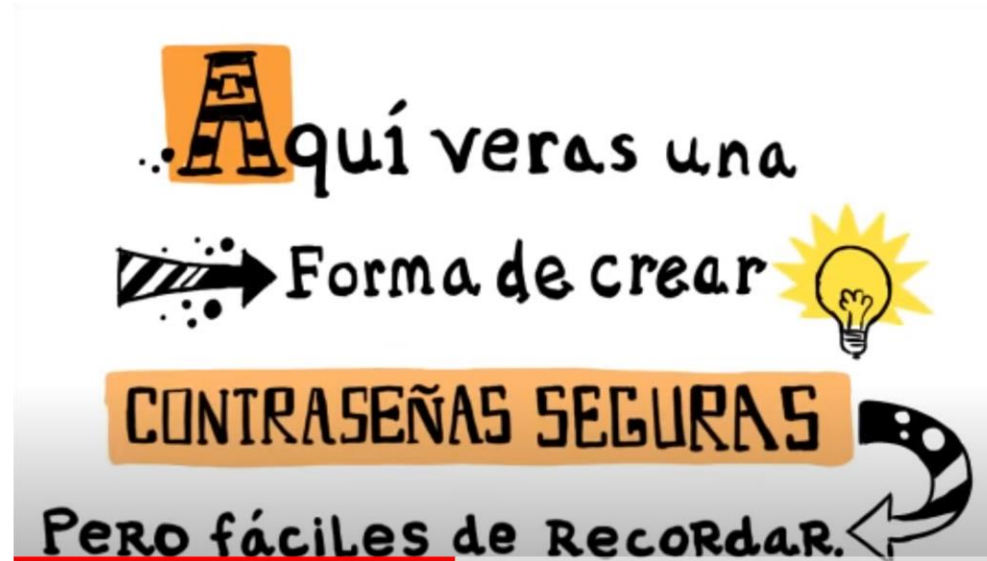
## Medidas de protección

**Lo que debes evitar...**



- Nombres propios de familiares, mascotas, amigos, lugares de origen o veraneo...
- La palabra “Contraseña” o “Password”.
- El nombre del servicio o aplicación.
- Hobbies y aficiones (Equipos de fútbol, artistas o grupos musicales, nombres de actores o películas, etc.).
- Números de teléfono o móvil, fechas, DNI...
- Palabras completas fácilmente adivinables.
- Secuencias alfanuméricas: 654321, 111111, A1B2C3D4...
- Secuencias de teclas próximas: qwerty, asdfgh, etc.
- Registrarte en sitios web con tus cuentas de otras aplicaciones/sitios.

## ¿Cómo crear una contraseña segura?



[http://youtu.be/iV9CmN-g\\_go](http://youtu.be/iV9CmN-g_go)

## Comprueba si tu contraseña es segura

### Comprueba tu contraseña

Tu contraseña no es segura si puede ser averiguada mediante un ataque de fuerza bruta o se encuentra en una base de datos de contraseñas filtradas.

No recopilamos ni almacenamos las contraseñas. [Más información](#)



Comprueba tu contraseña


.....



### ⚠ ¡Es hora de cambiar la contraseña!


- Tu contraseña se puede crackear fácilmente.
- ⚠ La contraseña es común o es una palabra
- Esta contraseña ha aparecido 767 veces en una base de datos de contraseñas filtradas.

<https://password.kaspersky.com/es/>

 Password Checkup

No se ha detectado ninguna de tus contraseñas recientes en una quiebra de seguridad de datos.

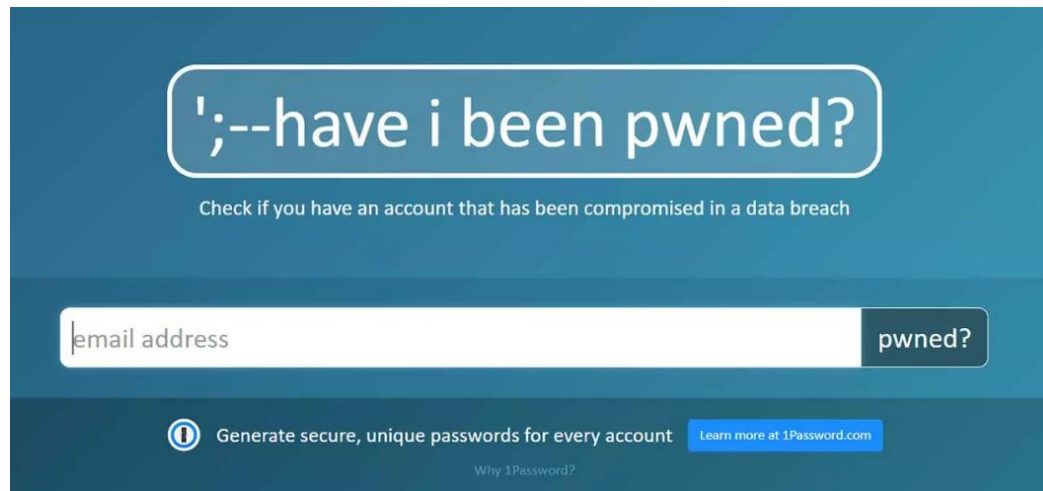
[Más información](#)

 [Configuración avanzada](#)

## Password Checkout

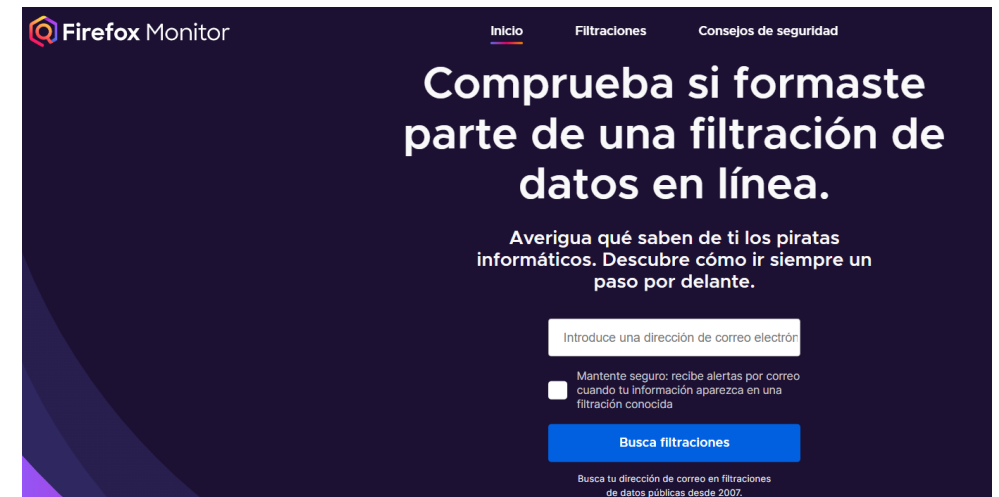


## Comprueba si tu contraseña ha sido robada



<https://haveibeenpwned.com/>

<https://monitor.firefox.com/>



## Autenticación de doble o múltiple factor

Es una capa adicional de seguridad que complementa el uso de una contraseña. Sirve para verificar la identidad de la persona.



### ¿Cómo?

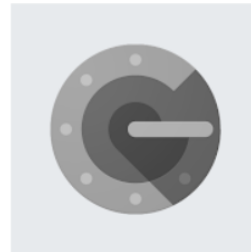
- Mediante llamada de teléfono o SMS.
- Usando datos biométricos (huella, reconocimiento facial).
- Con una tarjeta inteligente (token) física o virtual.

**¡RECUERDA!**

Actívalo en todos los servicios que lo tengan disponible o utiliza una aplicación que te lo permita.

# Medidas de protección

## Usa gestores de contraseñas



# CONTRASEÑAS



Secretas



Seguras



Únicas



Actualizadas

## ¿Cómo lograrlo?



Contraseñas robustas



Factor de autenticación múltiple



Gestores de contraseñas



# Ingeniería Social

# ¿Qué son?

Son ataques **basados en el engaño para conseguir que revelemos información personal que les sirva para acceder a nuestros dispositivos y/o cuentas.**



# Tipos de ataques

**Phishing** ✦ **Spear phishing** ✦ **Phishing basado en malware**  
**Vishing** ✦ **Smishing** ✦ **QRishing**



Recibimos mensajes generalmente urgentes o atractivos de entidades aparentemente legítimas (banco, red social, servicio técnico, entidad pública, etc.).

Enlace a una web fraudulenta

Archivo adjunto con malware

# Tipos de ataques

## Phishing



## Spear phishing



## Phishing basado en malware



## Vishing



## Smishing



## QRishing



## Medidas de protección



- **Sé precavido y lee el mensaje detenidamente, desconfía de peticiones urgentes, promociones o chollos demasiado atractivos.**
- **Presta atención al lenguaje, redacción, ortografía, gramática, etc.**
- **Antes de pinchar en el enlace verifica que la dirección a la que apunta sea la que debe ser.** Ingresa la URL directamente en el navegador (escríbela o búscala con tu navegador).
- **Comprueba el remitente del mensaje,** si es alguien conocido, comunícame con él por otro medio para confirmar el mensaje.
- **Si trae algún archivo adjunto, no lo descargues o analízalo previamente con un antivirus antes de abrirlo.**
- **En caso de llamadas, NUNCA des información personal o confidencial, ni sigas instrucciones extrañas.**
- **No contestes nunca al mensaje y elimínalo.**
- **No escanees códigos QR de procedencia desconocida, verifica que sean legítimos y utiliza una app que te permita ver previamente el enlace al que conduce.**

<https://www.osi.es/es/campanas/ingenieria-social/prueba-deteccion-ingenieria-social>

# Ejemplos

RV:WG: Tienes (1) documentos nuevos 5b62936506b4a !



La dirección de remitente debe corresponder con el dominio real.



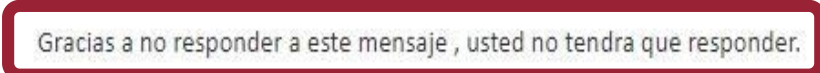
Adjunto sospechoso

**//ABANCA**

Estimado/a Cliente  
Deseamos informarle de que tiene una nueva actualización !



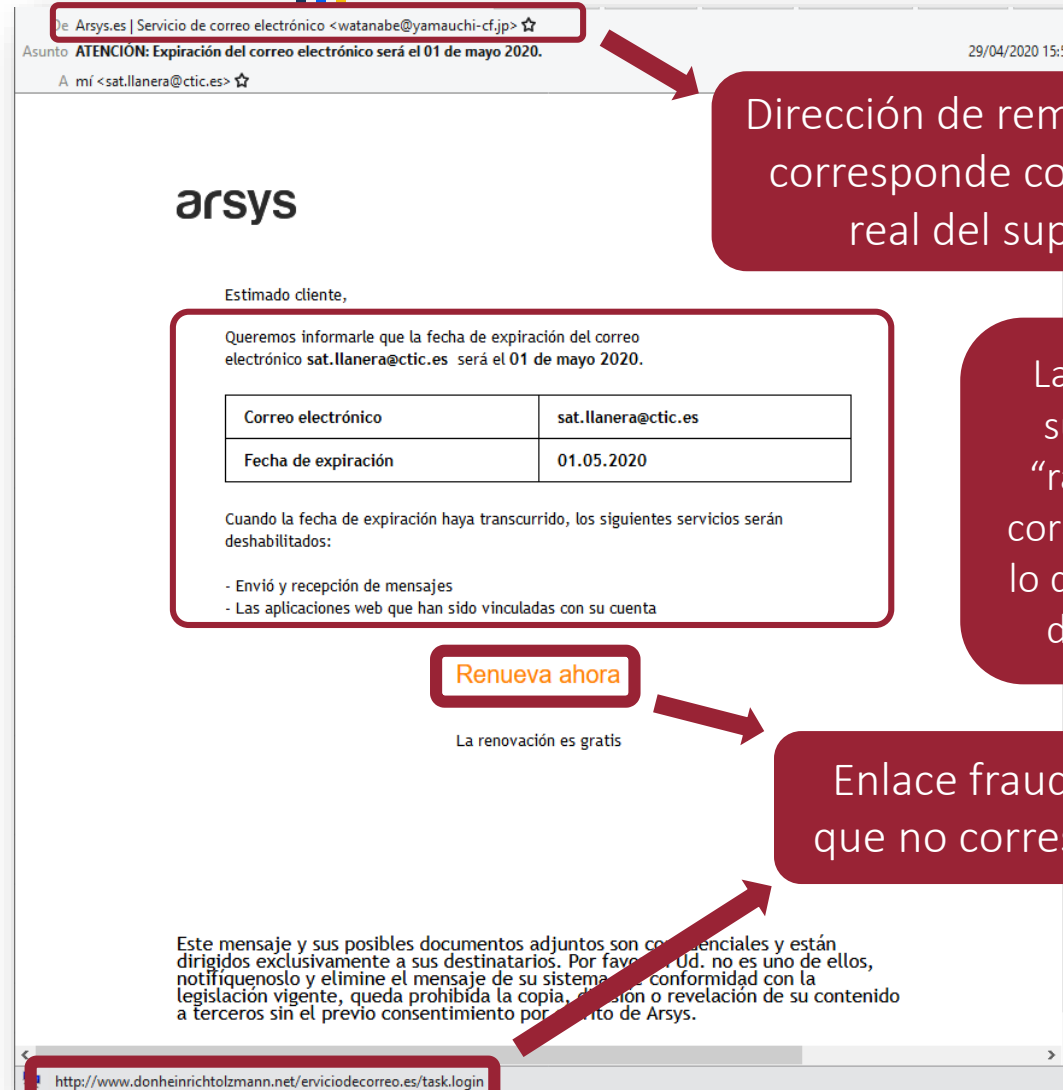
Si colocas el puntero del ratón encima podrás ver el enlace real



Atentamente,  
Director General : Francisco Botas

Redacción extraña

# Ejemplos



La información sobre el supuesto problema es "rara"; una dirección de correo concreto no expira, lo que expira es el servicio de correo contratado.

Enlace fraudulento, a URL que no corresponde a Arsys

## ¿Puedes detectar cuándo te están engañando?

La identificación de un ataque de suplantación de identidad (phishing) puede ser más difícil de lo que piensas. El phishing consiste en que un atacante intenta engañarte para que facilites tu información personal haciéndose pasar por alguien que conoces. ¿Podrías detectar qué es falso?

HACER EL TEST



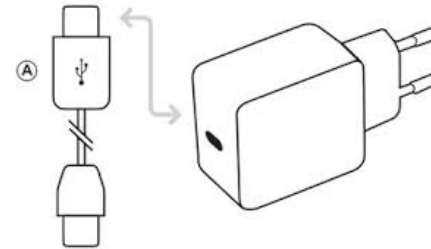
<https://phishingquiz.withgoogle.com/>



## Baiting “Gancho o cebo”



Se valen de un medio físico que utilizan para lograr que nosotros mismos infectemos nuestros dispositivos.



## Medidas de protección



- ✓ Evita conectar dispositivos desconocidos de almacenamiento externo o con conexión USB a tus equipos.
- ✓ Mantén tu sistema actualizado y las herramientas de protección, como el antivirus, activadas y actualizadas.

## Tipos de ataques

### Dumpster Diving “Buceo en basureros”



*Buscan en nuestra basura para obtener información sobre nosotros o la empresa que luego puedan utilizar para un ataque.*



## Medidas de protección



La única medida de protección es la **eliminación segura de información**, tanto si se encuentra en medios físicos como en medios digitales.

Para medios físicos su destrucción de manera irrecuperable y en medios digitales el formateo a bajo nivel es una buena opción.

## Fraudes online

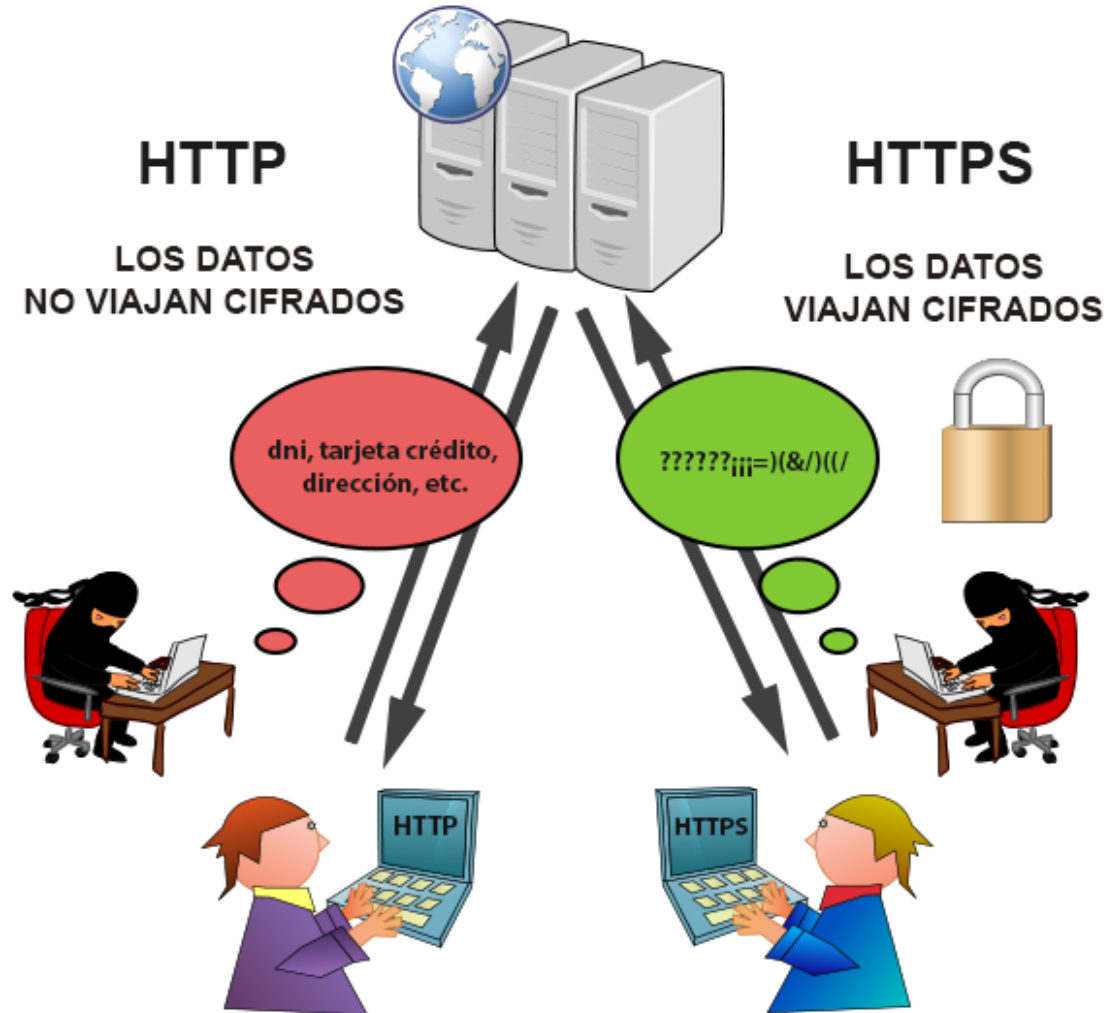


*(Fuente: Revista CISO)*

Son todo tipo de estafas online que usan para robarnos datos personales o dinero (falsos préstamos, tiendas online fraudulentas, falsos alquileres, falso soporte técnico, sextorsión, perfiles falsos, entre otros). Sus objetivos y medidas de protección varían de un tipo a otro.

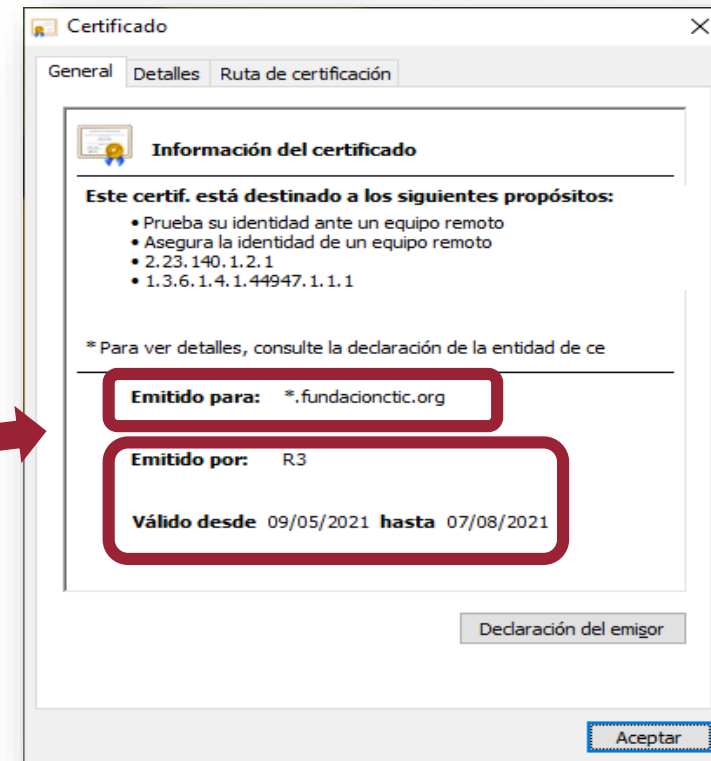
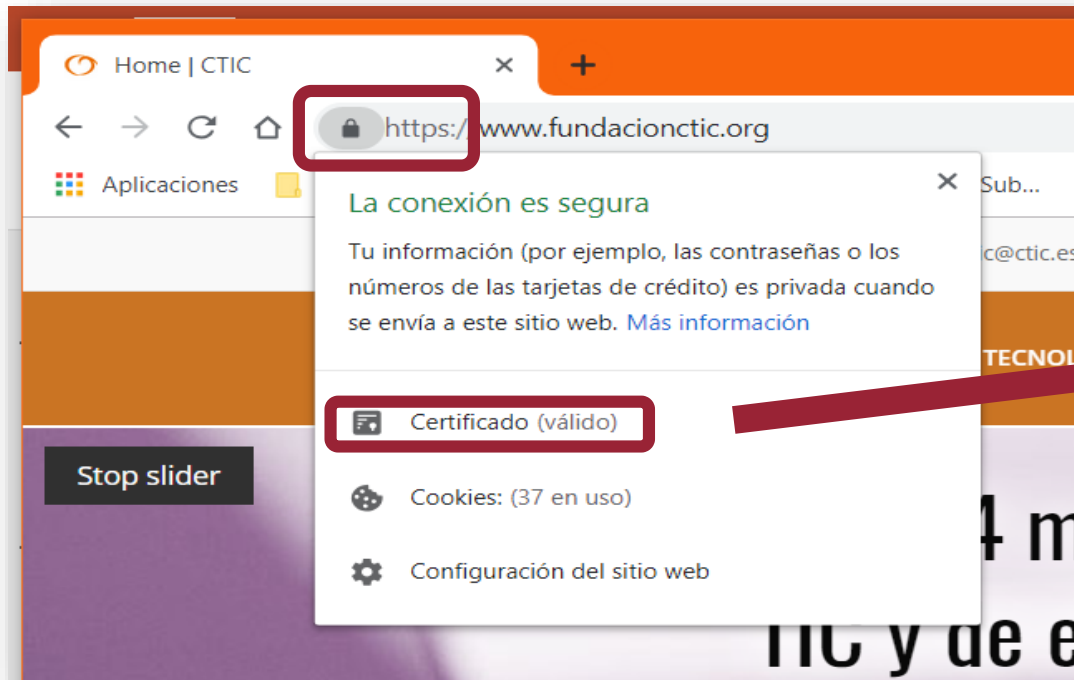
# Medidas de protección

**Navegación  
segura**



# Medidas de protección

**Certificado digital de seguridad (SSL)**  
Verifica los datos del certificado del sitio.



**¡RECUERDA!**

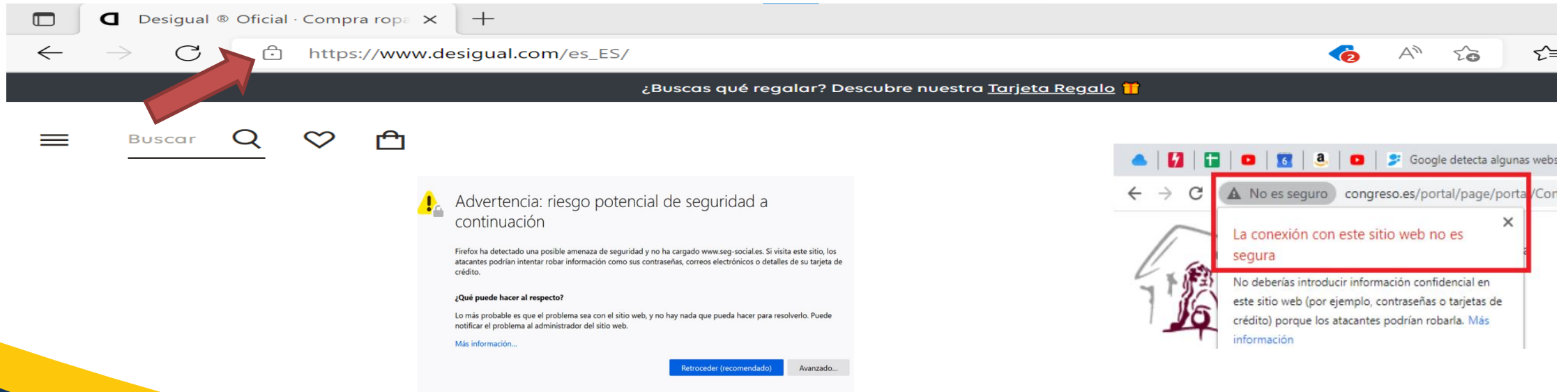
Siempre verifica la dirección web.

# Medidas de protección

## ¿Es una web segura?

### Barra de dirección:

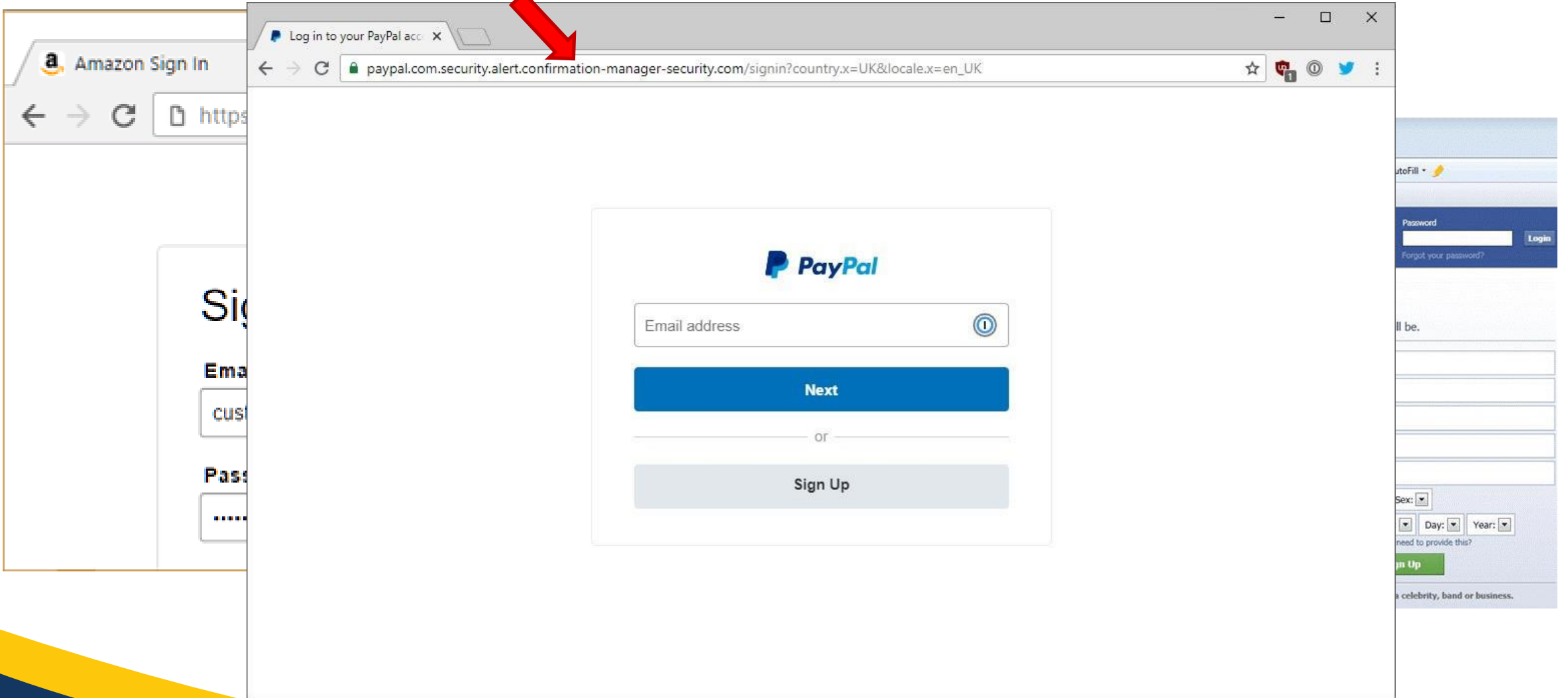
Mira la dirección del sitio y el tipo de certificado que contiene, si cuenta con el certificado de seguridad, tu navegador te lo mostrará. El dominio del sitio debería corresponder con el nombre de la marca o empresa (escrito correctamente) y relacionarse con el contenido.



The image shows two browser screenshots. The left screenshot shows a secure connection to [https://www.desigual.com/es\\_ES/](https://www.desigual.com/es_ES/). A red arrow points to the lock icon in the address bar. The right screenshot shows an insecure connection to [congreso.es/portal/page/portal/Cor](http://congreso.es/portal/page/portal/Cor). A red box highlights the warning message: "No es seguro" and "La conexión con este sitio web no es segura". Below the warning, it states: "No deberías introducir información confidencial en este sitio web (por ejemplo, contraseñas o tarjetas de crédito) porque los atacantes podrían robarla. Más información".



# Ejemplos



The image shows a browser window displaying a PayPal sign-in page. The address bar contains the URL: `paypal.com.security.alert.confirmation-manager-security.com/signin?country.x=UK&locale.x=en_UK`. The page features the PayPal logo at the top, followed by an "Email address" input field with an information icon. Below the input field is a blue "Next" button. Underneath the "Next" button is the word "or" and a grey "Sign Up" button. To the left, a partial view of an Amazon sign-in page is visible. To the right, a partial view of another sign-in page is visible, showing a "Password" field and a "Login" button. A red arrow points from the top of the image to the browser address bar.

## El contenido:

Mira el logo o imagen principal, que sean originales. Si los ves borrosos o con ligeras modificaciones, desconfía. Puedes verificarlo si lo descargas y lo buscas en Google para comprobar en qué otros sitios aparece.



### Buscar por imagen ×

Haz búsquedas en Google con una imagen en lugar de utilizar texto. Prueba a arrastrar una imagen aquí.

**Pegar URL de imagen** ? **Subir una imagen**

**Buscar por imagen**

# El comercio

# Medidas de protección

Debes mantener actualizados sistema operativo y aplicaciones y mantener optimizadas sus configuraciones.

## Tienda Online

 **Woo** **COMMERCE**



**PrestaShop**

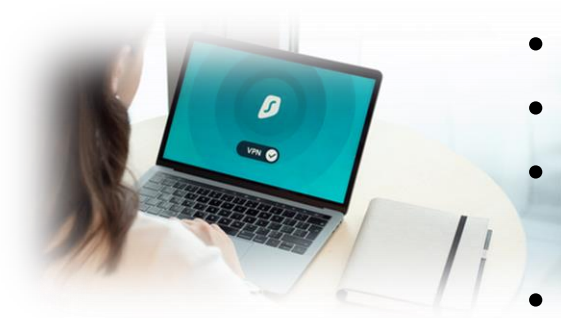
 **Magento**

 **shopify**

- ✓ Usa certificado SSL.
- ✓ Usa Pasarela de pago segura con varias alternativas de pago.
- ✓ Haz una correcta gestión de permisos de acceso o roles.
- ✓ Usa sistemas Captcha cuando tengas formularios.
- ✓ Ofrece información clara y concisa sobre los productos y sus condiciones de compra.
- ✓ Aporta a los clientes información sobre la política de privacidad de la empresa, aviso legal y política de cookies (requerido por LOPD).
- ✓ Cuida la privacidad de los datos del cliente solicitando sólo los datos necesarios.

## Operaciones de comercio electrónico

**Algunas alertas para detectar compradores fraudulentos:**

- 
- Datos del cliente erróneos o inconsistentes.
  - Varios clientes diferentes con la misma dirección de destino.
  - Solicitudes de envío urgente de pedido cuando este tipo de envío incrementa considerablemente el valor de la compra.
  - Varios intentos fallidos de compra en el TPV antes de que la compra sea aceptada.

# ¿Cómo actuar si has sido víctima?

## Ante la sospecha...



- No enviar nunca la mercancía.
- Contactar con el banco para comprobar que la transacción es correcta pidiendo una respuesta por escrito.
- Contactar con el cliente para que verifique los datos.
- Pedir que envíe sus datos personales por correo electrónico.
- Nunca usar el dinero proveniente de una posible compra fraudulenta ya que puede ser reclamado por la entidad emisora de la tarjeta.

**Y si has sido víctima, acudir a autoridades para interponer la denuncia.**

# Redes Sociales

# Medidas de protección

- Configura las opciones de privacidad, dejando poca información visible a desconocidos.
- Activa la autenticación o verificación en 2 pasos.
- No publiques determinados datos personales y familiares, especialmente fecha nacimiento, ubicación, domicilio, número de móvil y correo electrónico.
- Ten solo las aplicaciones necesarias con acceso a los perfiles y con los permisos indispensables.
- Abre solo enlaces seguros desde tus redes sociales, como desde cualquier otro sitio
- Extrema la precaución si interactúas con cuentas desconocidas.
- Usa los buscadores dentro de las redes sociales para encontrar información sobre archivos o mensajes sospechosos.
- Evita llenar formularios que prometan premios o dinero solo dando tu información.





# ¿Cómo actuar si has sido víctima?



## Algunas recomendaciones a tener en cuenta:

- ✓ Bloquea tus cuentas bancarias si pueden estar en riesgo.
- ✓ Informa a tus contactos.
- ✓ Si usas la misma contraseña en otros sitios cámbialas.
- ✓ Verifica si hay anuncios o aplicaciones en tu cuenta y bórralos.
- ✓ Denuncia en la red social afectada o afectadas.
- ✓ Denuncia a las autoridades.

# Software malicioso o “Malware”

# ¿Qué es?

Es un software que interfiere con el propósito de dañar al usuario del ordenador, **su objetivo es robar datos personales, financieros y/o comerciales.**

**Puede tomar la forma de código ejecutable, scripts, contenido activo y otro software.**

También puede encriptar o eliminar datos confidenciales, modificar o desviar las funciones básicas del ordenador, espiar la actividad informática de los usuarios.

## Tipos

- Virus informáticos
- Gusanos
- Caballos de Troya
- Software de rescate
- Spyware
- Adware
- Software de miedo, etc.





## Medidas de protección

- **Evita instalar aplicaciones innecesarias, si lo haces que sea en equipos de prueba o seguros** (sin conexión a la red interna, sin información sensible, con antivirus, etc.).
- **Evita la descarga de ficheros en los equipos que se usen en la actividad del negocio.**
  - ✓ Si lo haces, procura **hacerlo en un equipo sin información sensible.**
  - ✓ Procura **que ese equipo no esté conectado a la red de la empresa.**
- **Revisa con un antivirus los archivos descargados antes de abrirlos o ejecutarlos.**



# Protege tu Smartphone



# Medidas de protección

- Usa **bloqueo de acceso** (PIN, contraseña, medidas biométricas...).
- **Evita instalar aplicaciones fuera de la tienda oficial** y vigila los **permisos que otorgas** a las apps.
- **Mantén actualizados** tanto el SO como las apps.
- **Precaución al conectarse a enchufes USB públicos, o a dispositivos de terceros.**
- **Instala antivirus en los dispositivos que lo permiten.**





# Redes wifi



# Medidas de protección



- **Evita las redes abiertas**, las que no requieren autenticarse, en especial en lugares públicos (aeropuertos, estaciones, cafeterías...).
- **Verifica que se trata de la wifi auténtica** antes de conectar.
- Evita acceder a sitios que requieran ingreso de datos sensibles.

**Si tienes datos móviles mejor crea tu propio punto de acceso móvil cifrado.**

- **Desactiva el uso compartido de archivos.**
- **Navega en sitios seguros que utilicen cifrado HTTPS.**
- **Limita la actividad que realices mientras estés conectado, evita ingresar a sitios donde debas registrar datos confidenciales o personales.**



# Dispositivos de uso compartido



# Medidas de protección



- **Nunca guardes las contraseñas de acceso a servicios o aplicaciones.**
- **Cierra siempre la sesión** de cualquier servicio al que hayas accedido.
- **Borra** el historial de navegación, cookies y archivos temporales de internet del **navegador** que hayas utilizado.
- **Elimina cualquier archivo que se haya descargado** (y en el caso de ordenadores, vacía la papelera).
- **Elimina aplicaciones** que hayas instalado y que hayan podido sincronizar o almacenar información sensible.





# Sistemas de respaldo y planes de contingencia

# Copias de seguridad

## ¿Qué son?

- Es un proceso mediante el cual se **duplica la información existente de un soporte a otro.**
- En el **ámbito empresarial** se podría decir que es la **salvaguarda de nuestro negocio.**



# Copias de seguridad

## ¿Por qué hacerlas?

- La pérdida de información puede suponer la **pérdida de horas de trabajo** y podría tener graves **consecuencias para la continuidad del negocio**.
- Los soportes (discos duros externos/internos, pendrive, etc.) donde guardamos esa información suelen tener una **vida útil limitada (averías, desgastes...)** y están sujetos a diversos **riesgos y/o amenazas (accidentes, ataques...)**.





# Copias de seguridad

## Antes de Realizarlas

Mantén organizada tu información y clasifica la que se guardará, de acuerdo a diferentes criterios:

» **por el nivel de accesibilidad o confidencialidad:**

- Confidencial: accesible solo por la dirección o personal concreto.
- Interna: accesible solo al personal de la empresa.
- Pública: accesible públicamente.

» **por su utilidad o funcionalidad:**

- Información de clientes y proveedores.
- Información de compras y ventas.
- Información de personal y gestión interna.
- Información sobre pedidos y procesos de almacén.

» **por el impacto en caso de robo, borrado o pérdida:**

- Daño de imagen.
- Consecuencias legales.
- Consecuencias económicas.
- Paralización de la actividad.



- Periodicidad.
- Tipo de soporte.
- Disposición física del soporte.

## Espejo “Mirror Backup”

Es una copia exacta de los datos originales. Se suele hacer “en directo”, es decir, a la vez que trabajas con los datos reales, se hace una copia espejo en un disco alternativo.

Ventajas	Desventajas
La restauración es muy ágil.	Si un archivo se elimina accidentalmente en el sistema original, el sistema espejo lo elimina también.
No contiene archivos antiguos o en desuso.	
Se hace en tiempo real.	

## Completa “Full Backup”

Copia de todos los datos de nuestro sistema.

Ventajas	Desventajas
Fácil restauración de los datos, ya que todos los datos han sido copiados.	Mayor necesidad de espacio de almacenamiento. Información redundante.
	Mayor tiempo para hacer la copia.
	No es recomendable realizar una copia completa en horario laboral.
	Coste elevado.



## Incremental “Backup Incremental”

La única copia completa es la primera. A partir de ahí, las copias posteriores sólo almacenan los cambios realizados desde la copia de seguridad anterior.

Ventajas	Desventajas
El proceso de hacer la copia de seguridad es mucho más rápido.	El proceso de restauración es más largo porque tienes que utilizar varias copias diferentes para restaurar completamente el sistema.
Ocupa menos espacio de almacenamiento = menos costo.	

## Diferencial “Backup Diferencial”

Similar a una copia incremental en la primera vez que se lleva a cabo. Sin embargo en las siguientes copias , no solo se copiarán los datos que se hayan modificado desde la última copia, sino todos los que se hayan modificado desde la última copia completa realizada.

Ventajas	Desventajas
El tiempo de restauración es menor.	Requiere más espacio que las copias incrementales.
Solo hay que comprobar su existencia en 2 copias de respaldo.	El tiempo que tarda en hacerse desde que inicia hasta que termina es considerable.

# Tipos de copias de seguridad



# ¿Dónde almaceno mis copias de seguridad?

El soporte escogido depende de la cantidad de información que necesitemos conservar, del sistema de copia elegido y de la inversión que deseemos realizar.

- Pendrives???
- Discos duros (HDD y SSD).
- Discos ópticos: la utilización de blu-rays como dispositivos de almacenamiento.
- La nube (Drive, OneDrive, DropBox, etc.)
- Dispositivos NAS (del inglés Network Attached Storage).
- Cintas magnéticas DAT/DDS (Digital Audio Tape/Digital Data Storage) / LTO (Linear Tape-Open).



# ¿Cómo almaceno mis copias de seguridad?

## La estrategia 3-2-1

- 3: Mantener 3 copias de cualquier fichero importante: el archivo original y 2 backups.
- 2: Almacenar las copias en 2 soportes distintos de almacenamiento para protegerlas ante distintos riesgos.
- 1: Almacenar 1 copia de seguridad fuera de nuestra empresa.



Crear **3** copias de los datos (1 original y dos secundarias)



Al menos **2** tipos de formatos de almacenamiento distintos

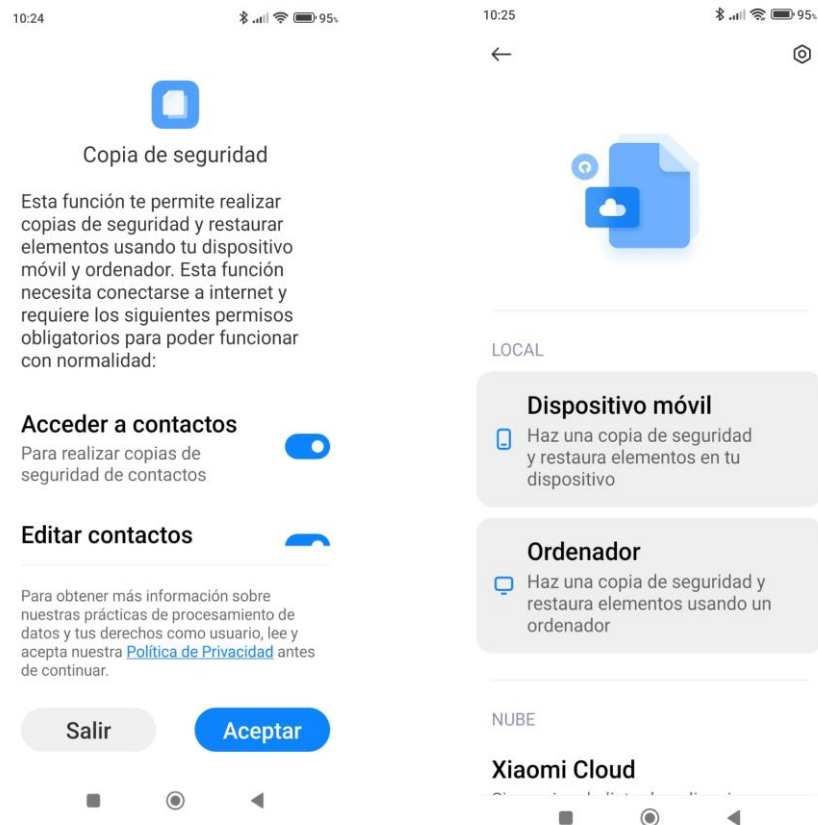


Almacena **1** fuera del lugar de trabajo

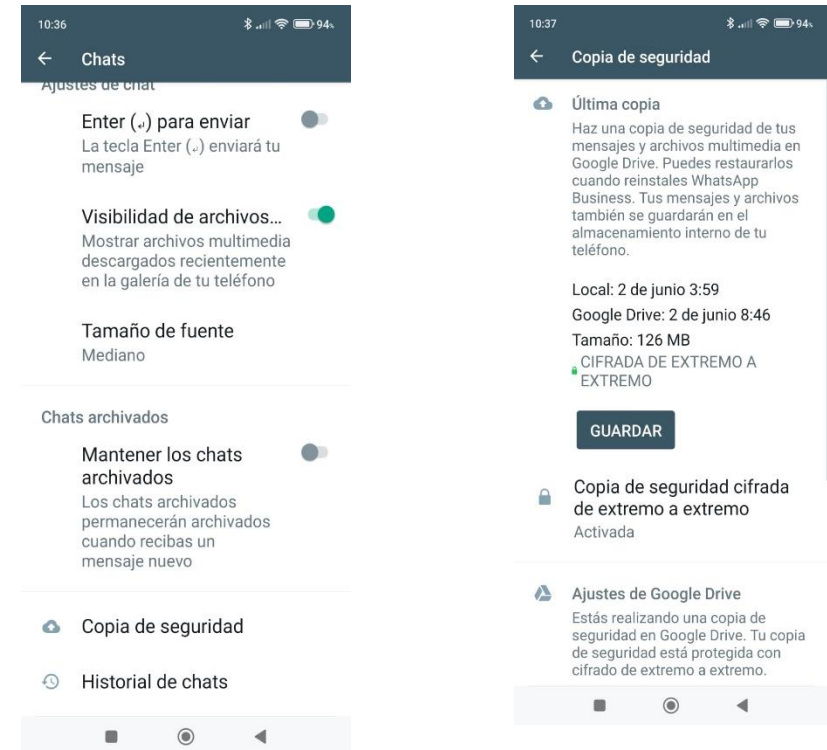


# ¿Y el Smartphone?

## Dispositivos



## Aplicaciones





DIGITALIZACIÓN • COMERCIO • ASTURIAS





DIGITALIZACIÓN • COMERCIO • ASTURIAS

