



Guía básica de **ciberseguridad**

en lectura fácil



Subvencionado por la Junta de Castilla y León con cargo a la asignación tributaria del IRPF

Creación y adaptación de los contenidos a lectura fácil según la norma UNE 153101:EX 2018

Validación

Centro San Juan de Dios (Valladolid)

Asprosub Benavente (Zamora)

Edita:

Plena inclusión Castilla y León

 Plena inclusión Castilla y León

Índice

1. ¿Qué es la ciberseguridad?	Página 5
2. Cómo proteger tus dispositivos	Página 6
3. Protege tus cuentas e información	Página 18
4. Conéctate de forma segura a Internet	Página 23
5. Detecta engaños	Página 32
6. Seguridad en redes sociales	Página 43
7. Seguridad en compras y descargas	Página 51
8. Hacer copias de seguridad	Página 54
9. Test final	Página 58
10. Diccionario	Página 60

El manual está escrito en lectura fácil.

La lectura fácil es una forma de escribir que sigue unas normas para que las personas con dificultades de comprensión puedan entender lo que leen.

En este documento vas a encontrar palabras difíciles de entender. Estas palabras están en **negrita**.

Al final de cada página vas a encontrar unos cuadros que explican el significado de estas palabras.

Estos cuadros se llaman glosas.

Además, estas palabras y otras importantes están al final en un diccionario que puedes consultar siempre que lo necesites.

Esta guía usa a veces las palabras en masculino y otras en femenino para cumplir con criterios de lenguaje inclusivo.

¿Qué es la ciberseguridad?

La ciberseguridad es proteger dispositivos y la información que hay en ellos de ataques informáticos.

La ciberseguridad es muy importante porque cada vez tenemos más información en nuestros dispositivos como teléfonos, ordenadores o tablet.

En este manual vas a conocer algunas medidas de ciberseguridad para poder navegar y utilizar dispositivos de forma segura.



Protege tus dispositivos

1. Cómo proteger tus dispositivos

Los dispositivos son aparatos informáticos que hacen una tarea.

Por ejemplo: un ordenador, un móvil o una tablet.



Hay varias formas de proteger tus dispositivos:



- 1.Actualizar tus dispositivos
- 2.Instalar un antivirus
- 3.Bloquear el acceso

A continuación vas a ver cómo hacerlo.

Actualizar tus dispositivos

Actualizar un dispositivo significa descargar la última versión del sistema operativo.

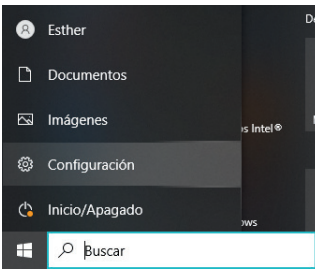
El sistema operativo es el programa básico que tiene que tener un dispositivo para poder funcionar y hacer tareas en él.

¿Cómo actualizar tu sistema operativo?



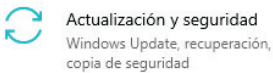
Paso 1.

Haz clic en el icono de Windows y después haz clic en “Configuración”.



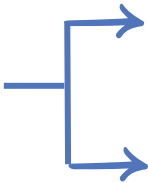
Paso 2.

Haz clic en “Actualización y seguridad”.



Paso 3.

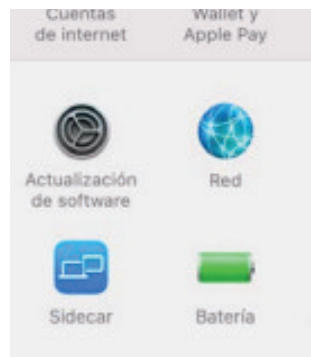
En la siguiente pantalla podrás ver si tienes la última versión de Windows.





Paso 1.

‘Entra en el menú de Apple.
Después pincha en “Preferencias del Sistema”
y en “Actualización de software”.
Allí te dirá si está actualizado
o tienes que hacerlo.



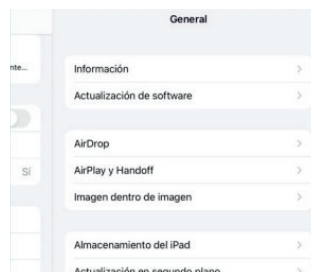
Paso 2.

Si quieres que el ordenador busque solo
las actualizaciones
pincha en la casilla “Mantener mi MAC actualizado”.



Paso 1.

Entra en “Ajustes”, pincha en “general”
y busca la opción
“Actualización de software”.
Allí te dirá si está actualizado
o tienes que hacerlo.



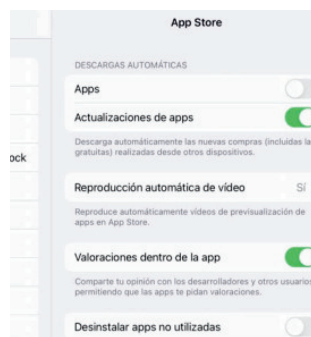
Paso 2.

Si quieres que el teléfono busque solo
las actualizaciones
pincha en la casilla
“Mantener mi MAC actualizado”.



Paso 3.

Si quieres actualizar todas las aplicaciones
entra en “Ajustes” y pincha en “App Store”.
Allí activa la función “Actualizaciones de apps”.



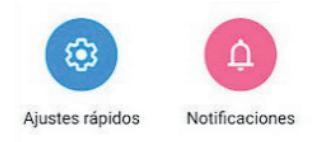


En Android

Paso 1.

Pincha en “Ajustes”.

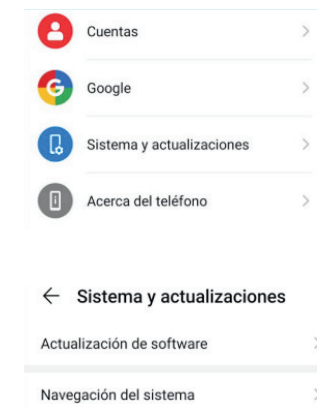
Después pincha en “Información del dispositivo”
en “Ajustes avanzados”
y por último en “Actualizaciones del sistema”.



Paso 2.

Pincha en “Comprobar actualizaciones”
para ver si hay actualizaciones disponibles.
Si hay nuevas actualizaciones puedes descargarlas

Después pincha en “Sistema”
en “Ajustes avanzados”
y por último en “Actualizaciones del sistema”.



Instalar un antivirus

Un **antivirus** es un programa que protege nuestros dispositivos de virus y otras amenazas.

¿Dónde puedes descargar un antivirus?

Tienes que pagar dinero por la mayoría de programas de antivirus. Pero hay algunos que son gratuitos. En la página web del INCIBE tienes varios enlaces a antivirus gratuitos. También puedes acceder en este código QR.



El INCIBE es el Instituto Nacional de Ciberseguridad. Pertenece al Gobierno de España y tiene como misión enseñar a la ciudadanía cómo proteger mejor sus dispositivos y sus cuentas en Internet.

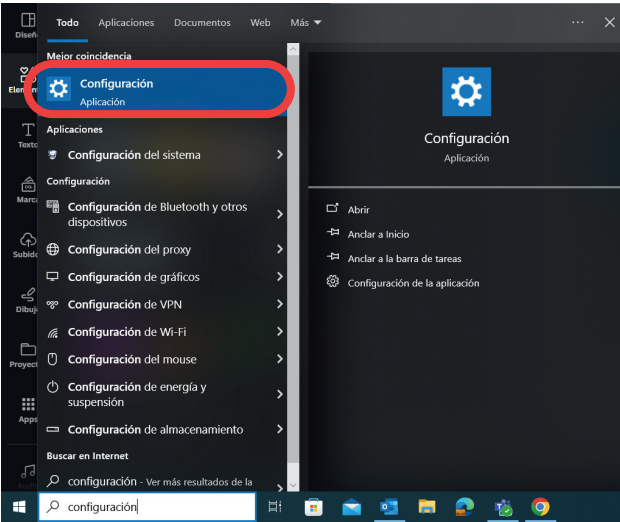


¿Cómo saber si tienes antivirus?

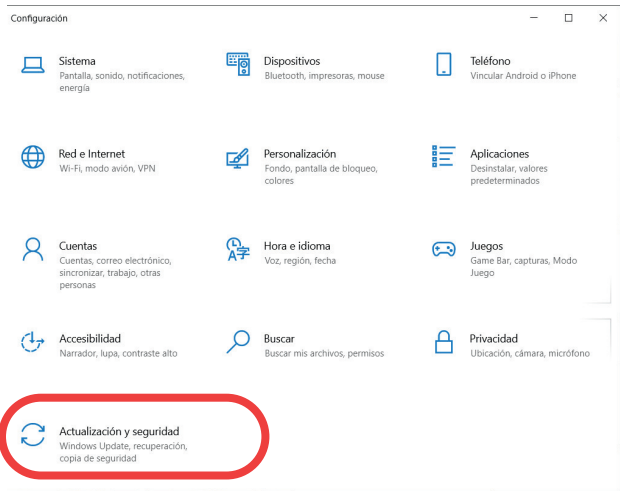
Ve al menú de Windows y pincha en configuración. Después pincha en actualización y seguridad.

Pincha en seguridad de Windows y después en protección contra virus y amenazas. Allí verás si has activado el antivirus o no.

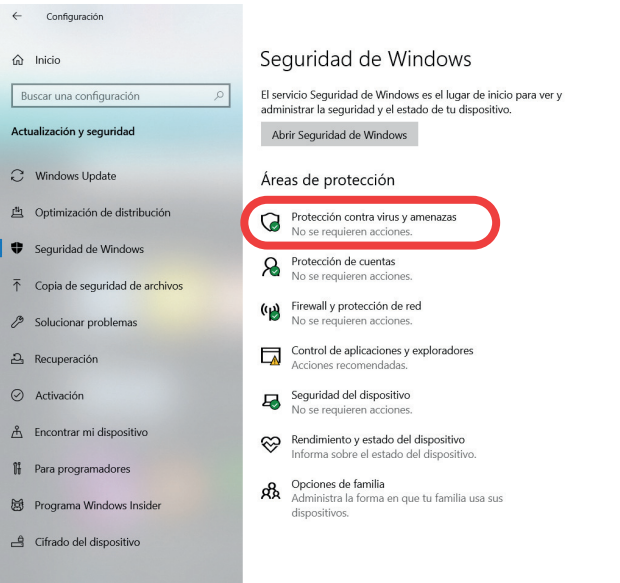
Paso 1.



Paso 2.



Paso 3.



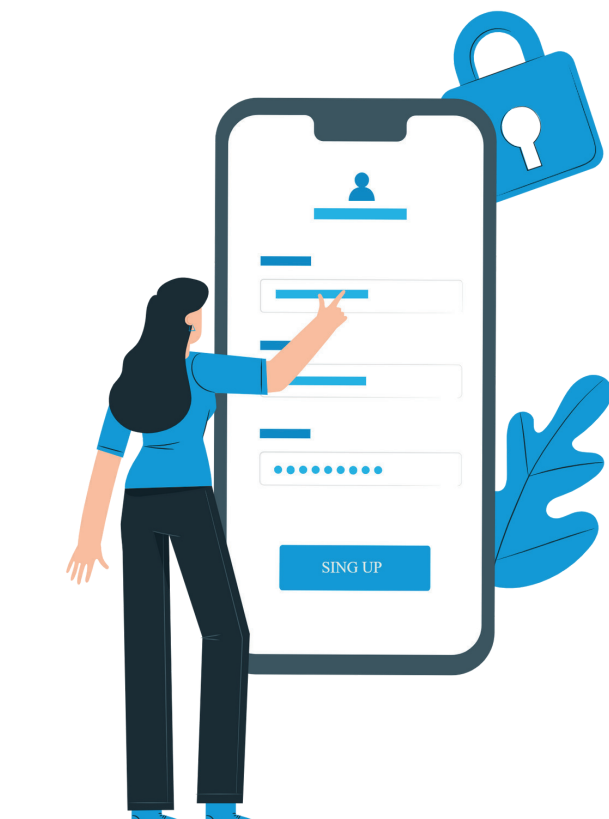
Bloquear el acceso

Una medida básica de ciberseguridad es bloquear el acceso a nuestros dispositivos. Eso significa poner una clave o un código para que solo pueda acceder al dispositivo su dueño.

Bloquear el móvil

Los tipos de bloqueo de acceso son:

- **Clave PIN.**
Código formado por 4 números.
- **Patrón.**
Dibujo que se hace uniendo hasta 9 puntos puestos en forma de cuadrado.
- **Huella dactilar.**
Hay teléfonos que tienen un sensor para detectar la **huella dactilar** de las personas usuarias.
- **Contraseña.**
Es una clave compuesta por números y letras.
- **Desbloqueo facial.**
El móvil reconoce nuestra cara a través de nuestra cámara.
- **Bluetooth.**
A través de una pulsera inteligente, móvil o tablet.



Huella dactilar

Es la huella de los dedos. Identifica a una persona porque ninguna huella es igual a la otra.

Bluetooth

Es una tecnología para conectar dispositivos que están a poca distancia.

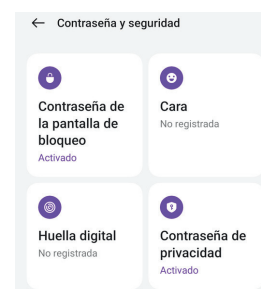
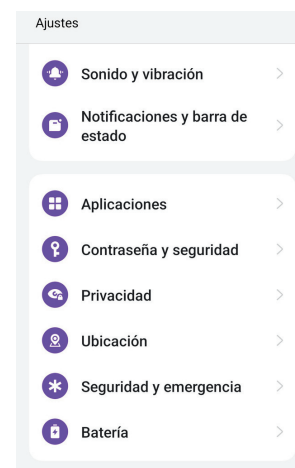


En Android

Paso 1.

Pincha en “Ajustes”.

Después pincha en “Contraseña y seguridad”.

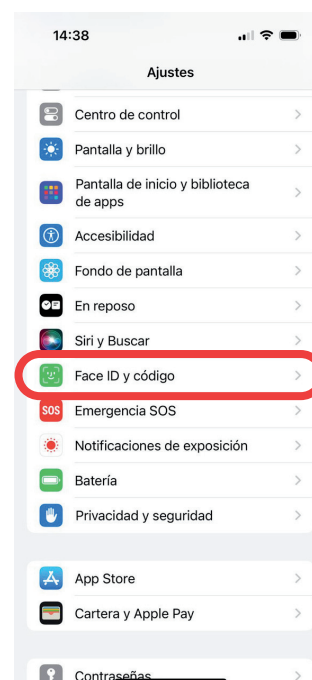


En iOS

Activar formas de bloqueo

Entra en “Ajustes”,

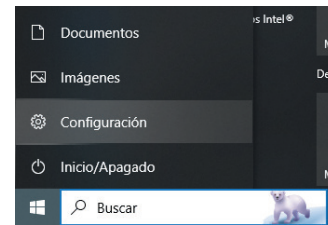
pincha en “Face ID y código”.





Paso 1.

Pincha en el icono de Windows y después pincha en “Configuración”.



Paso 2.

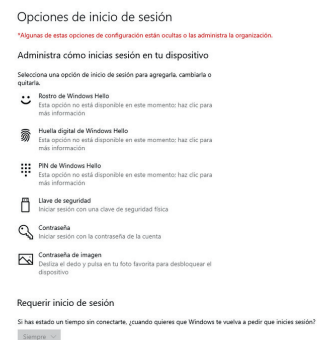
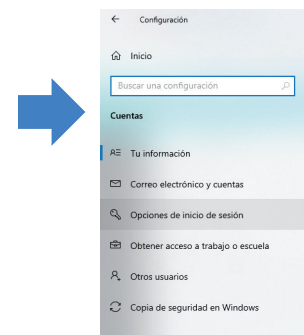
Pincha en “Cuentas” y en “Opciones de inicio de sesión”



Paso 3.

Selecciona alguna de estas opciones. Recuerda que no todos los ordenadores tienen todas las opciones:

- **Rostro de Windows Hello.**
Usa tu cara para iniciar sesión.
- **Huella digital.**
Inicia sesión con tu huella.
- **PIN de Windows Hello.**
Es un código de 4 números.
Es la opción menos segura.
- **Clave de seguridad.**
Es una clave física que está dentro de otro dispositivo, por ejemplo un USB.
Necesitas conectarlo al ordenador.





En MacOS

En versiones más modernas los ordenadores tienen instalado “TouchID”. TouchID es un sensor que tiene el ordenador para detectar tu huella. Para activarlo tienes que seguir estos pasos:

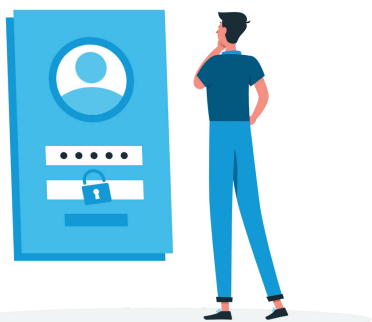
Paso 1

Ve al menú de Apple y pincha en “Preferencias del sistema”. Después selecciona “TouchID”.

Paso 2

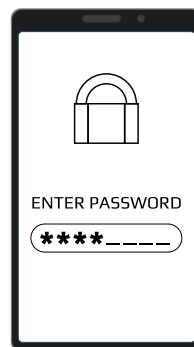
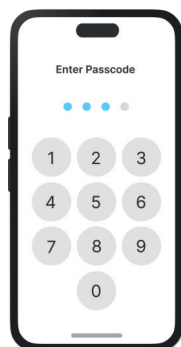
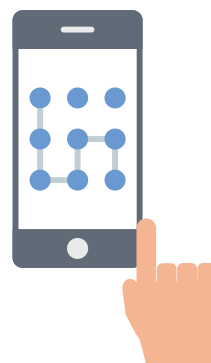
Pincha en “Añadir huella” y sigue las instrucciones.





Actividad

Escribe debajo de cada imagen
qué tipo de bloqueo es



Protege tus cuentas e información

1. Crea contraseñas seguras

Una contraseña es un conjunto de letras y números secretos. Es importante que pongas contraseñas seguras a tus dispositivos y cuentas.

Pasos para crear contraseñas seguras

- 1 Piensa una frase que tenga mínimo 10 letras.**
Ejemplo: **Esta es mi contraseña**
- 2 Pon la primera letra de cada palabra en mayúscula.**
Ejemplo: **EstaEsMiContraseña**
- 3 Sustituye algunas letras por números.**
Puedes sustituir la letra “i” por el número 1, la letra “e” por el número 3, la letra “a” por el número 4 o la letra “o” por el número 0.
Ejemplo: **3st43sM1C0ntr4s3ñ4**
- 4 Añade símbolos.**
Ejemplo: **3st43sM1C0ntr4s3ñ4!%**
- 5 Personaliza tu contraseña para cada uso.**
Ejemplo de contraseña para tu correo electrónico:
CE3st43sM1C0ntr4s3ñ4!%



Además tienes que seguir estos consejos:

- **Usa gestores de contraseñas.**
Los gestores de contraseñas son aplicaciones que guardan nuestras contraseñas de forma segura.
- **Usa contraseñas diferentes.**
Así te asegurarás de que si te roban una contraseña no pueden entrar en todas tus cuentas.
- **Cambia tus contraseñas.**
Cambia las contraseñas al menos cada 3 meses.
- **No compartas tus contraseñas.**
No le envíes ni digas tus contraseñas a nadie.



Actividad

Marca si los siguientes ejemplos son contraseñas seguras o no.

Miperrotoby	☒	☐
Hola1234	☒	☐
M1P3rr0S3Ll4m4T0by35%	☒	☐
micorreo	☒	☐
3M1C0rr30d3Gm4lI&	☒	☐



2. La verificación en dos pasos

La verificación en dos pasos es una medida de seguridad para hacer que sea más difícil que alguien entre a nuestras cuentas.

Cuando activamos la verificación en dos pasos tenemos que meter esta información:

1. Tu contraseña.
2. Un código que se envía a nuestro móvil y que solo funciona de forma temporal.

Hay aplicaciones que ya incluyen esta verificación. Si quieres poner la verificación en todas tus cuentas puedes descargarte estas aplicaciones:



Google authenticator



Microsoft authenticator

Mira cómo usar estas aplicaciones en este vídeo del INCIBE.





Actividad

Marca si las siguientes frases son verdaderas o falsas

La verificación en dos pasos es una medida de seguridad



Con la verificación en dos pasos
tienes que escribir un solo código



Todas las aplicaciones tienen verificación en dos pasos



Activas la verificación en dos pasos
para entrar más rápido a las aplicaciones



Hay aplicaciones para poner la verificación en dos pasos
en todas tus aplicaciones



Conéctate de forma segura a Internet



1. Navegar en modo privado

El modo privado es una opción que puedes activar en tu navegador. Esta opción sirve para que tu navegador no guarde información como el **historial**, contraseñas, las **cookies** o la información de formularios. También se llama modo incógnito.

Algunas ventajas del modo privado

- Evitas que se guarden tus datos personales o los datos de las tarjetas del banco.
- Si usamos el ordenador de otra persona no se guarda lo que hemos hecho o visto.

Algunas desventajas del modo privado

- Las páginas web detectan tus visitas y el código de tu conexión.
- No te protege de posibles virus o amenazas.



Aunque actives el modo privado, recuerda no eres invisible en Internet. Las páginas web registrarán tu visita.



Historial

Es la lista de páginas web que has visitado.

Cookies

Son archivos que tu ordenador guarda cuando visitas una página web.

¿Cómo activar el modo privado?



En Google Chrome

Pulsa en el menú o icono de 3 puntos arriba a la derecha y selecciona “nueva ventana de incógnito”..



En Mozilla Firefox

Pulsa en el menú o icono de 3 líneas arriba a la derecha y selecciona “nueva ventana privada”..



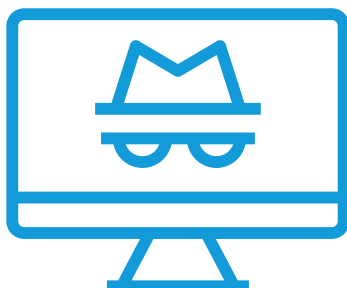
En Safari

Pulsa en las opciones de configuración y pincha en “navegación privada”.



En Edge

Pulsa en el menú o icono de 3 puntos arriba a la derecha y selecciona “nueva ventana InPrivate”.



Actividad

Marca si las siguientes frases son verdaderas o falsas

Cuando navegas en modo privado tu navegador no guarda tu historial	☒	☐
Con el modo privado no entran virus	☒	☐
El modo privado no guarda los datos de tu tarjeta del banco	☒	☐
El modo privado guarda la información de formularios	☒	☐

2. Identifica si una web es fiable



Es habitual que los delincuentes creen páginas web falsas parecidas a las originales para engañarnos.

Es importante que sepas identificar una web fiable y una web falsa.

Pasos para identificar páginas web falsas

1 Revisa el enlace de la web.

A veces las web falsas añaden o cambian letras.
www.plen0inclusioncyl.org

2 Revisa si usa una conexión segura.

Las web seguras empiezan por “https”.

3 Revisa si tiene certificado de seguridad.

Lo sabrás si al lado de la dirección hay un icono de candado.



4 Revisa el aspecto de la web.

Algunas web están mal traducidas o tienen imágenes de mala calidad o no tienen un aspecto cuidado.

5 Busca la información clave

Por ejemplo: quién es la persona propietaria o la información legal.
Esta información suele estar en la parte de abajo.

3. Conéctate a una red wifi de forma segura

Las redes wifi públicas no son seguras.
porque cualquier persona
puede robar nuestros datos.
Por ejemplo: nuestras contraseñas, archivos,
o nuestros mensajes.

Si estás fuera de casa
es mejor que uses la conexión de datos de tu móvil
para conectarte a Internet.

Recomendaciones para conectarte con seguridad fuera de casa

1 Comprueba que la red es oficial

Mira bien el nombre de la red
y comprueba con las personas de información
si es el nombre de la red oficial.

2 No compartas información

No entres en tu correo o en páginas
donde tienes que poner tu usuario y contraseña.

3 Actualiza tu dispositivo y las aplicaciones

Evitas tener fallos y debilidades.

4 Tener un antivirus

Así puedes eliminar virus
de tu dispositivo.

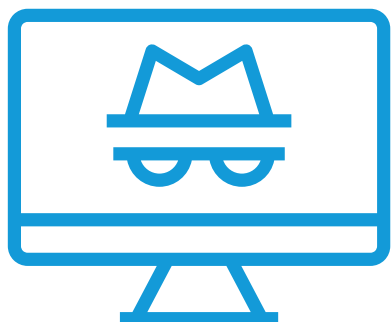
5 Navega por páginas web seguras

Las páginas web seguras son
las que empiezan por HTTPS
y tienen certificado de seguridad.

6 Navega de forma privada

De esta forma el navegador
no guarda la información
de lo que has visitado.





Actividad

Entra en tu navegador en la web
del Banco Santander
y explica por qué es una web segura.

4. Eliminar las cookies

Las **cookies** son los archivos que tu ordenador guarda cuando visitas una página web.

Cookies

Son archivos que tu ordenador guarda cuando visitas una página web.

¿Para qué sirven?

- Sirven para conocer tus hábitos cuando navegas en Internet.
- Recordar tus datos de acceso.
- No enseñarte información que ya ha aparecido.

¿Qué información recogen?

- Tu idioma
- Tipo de dispositivo
- Tu sistema operativo
- El tamaño de tu pantalla
- Qué navegador usas
- Tus contraseñas
- Las páginas web que has visitado.

Es recomendable eliminar de vez en cuando estos datos cada poco tiempo.





En Google Chrome

Paso 1

Entra en el menú de Google Chrome y haz clic en “Configuración”.

Paso 2.

Pincha en “Privacidad y seguridad” y después en ‘Cookies y otros datos de sitio’.

Paso 3.

Pincha en “Ver todas las cookies y datos de sitios webs” y selecciona “Eliminar todo”.



En Mozilla Firefox

Paso 1

Entra en el menú de Mozilla Firefox y haz clic en “Ajustes”.

Paso 2.

Pincha en “Privacidad y seguridad” y después en “Cookies y datos del sitio”.

Paso 3

Pincha en “Administrar datos” y después pincha “Eliminar todo”.



En Safari

Paso 1

Pincha en “Safari”,
después en “Preferencias” y “Privacidad”.

Paso 2

En el apartado “Cookies y otros datos de sitios web”
pincha en “Eliminar todos los datos de los sitios web”.



En Microsoft Edge

Paso 1

Entra en el menú de Microsoft Edge
y haz clic en “Configuración”.

Paso 2

Después pulsa en “privacidad, búsqueda y servicios”
y después en “Borrar datos de exploración”.

Paso 3

Pincha “Elegir lo que se debe borrar”
y las fechas de los archivos.
Por último, pincha en “Borrar ahora”.

Detecta engaños

Ingeniería social

Son las técnicas de engaño que usan las personas **delincuentes** para conseguir:

- Nuestros datos personales.
Por ejemplo: nuestras claves o número de tarjeta del banco.
- Descargar programas que pueden tener virus
- Visitar una página web que no quieres y que puede tener virus.

Las técnicas de ingeniería social más usadas son:

- Hacerse pasar por una marca de confianza o por alguien que conoces.
- Hacerse pasar por alguna oficina del Gobierno o un organismo oficial.
- Decirte que algo es muy urgente o que estás en peligro.
Por ejemplo: tienes un virus o un familiar ha perdido su móvil y la cartera y necesita que le envíes dinero.
- Te envían causas sociales falsas.
Por ejemplo: que recogen firmas para una causa o te piden hacer una encuesta.

Ingeniería social

Son las técnicas de engaño que usan los delincuentes para conseguir información.

Delincuentes

Personas que cometen un delito.
Por ejemplo: robar

7. Detectar peligros en Internet

En Internet hay mucha información y con mucho valor, pero también hay peligro de sufrir un **fraude**.

Un fraude es un delito en el que una persona engaña a otra para conseguir un **beneficio**.

En este caso, dinero o información.

Principales fraudes de ingeniería social



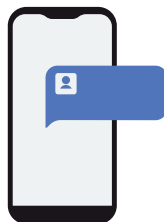
Phishing

Son correos que se hacen pasar por alguien conocido o por una empresa para robar tus datos.



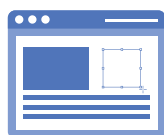
Vishing

Son llamadas que se hacen pasar por empresas, bancos o servicios técnicos para engañar a las personas y conseguir sus datos o controlar sus dispositivos.



Smishing

Son mensajes de texto o SMS que se hacen pasar por empresas, bancos o personas conocidas para engañar a las personas y conseguir sus datos o controlar sus dispositivos.



Páginas web falsas

Páginas web que se hacen pasar por empresas o negocios reales para conseguir información.



Fraude

Un delito en el que una persona engaña a otra para conseguir un beneficio.

Beneficio

Mejora que una persona recibe. Por ejemplo: dinero.



Baiting o “cebo”

Las personas atacantes dejan un USB infectado con virus en un sitio público para que una persona lo meta en su ordenador y puedan robar su información.

También usan anuncios en páginas web de concursos y premios falsos para que las personas pinchen en ellos y les roben su información.



Actividad

Une con una flecha cada palabra con su definición

Phising

Imita a páginas web reales para conseguir información

Vishing

Usa los SMS para engañar

Smishing

Usa un correo electrónico falso.

Páginas web falsas

Llama a personas para hacerse pasar por otras.



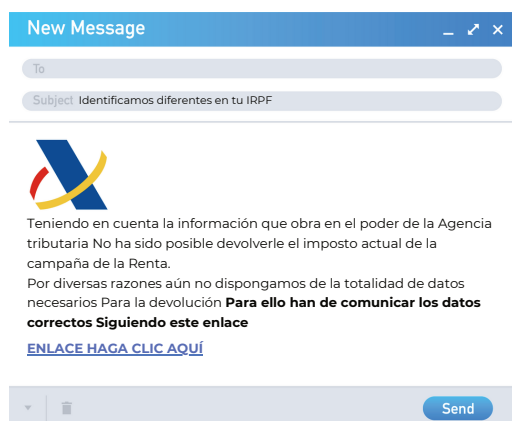
Descarga el juego “Detecta el fraude” del INCIBE ¡y aprende jugando!.





Actividad

Escribe debajo de cada imagen
qué tipo de fraude es



Cómo descubrir estos fraudes por mensaje

Revisa quién te envía el mensaje

Fíjate si te llama o escribe un número desconocido o una dirección de correo sospechosa.

Revisa el asunto

Suelen usar asuntos llamativos.

Pon atención a qué te piden

Piensa en que tu banco u otras empresas ya tienen tus datos.
Estos mensajes suelen pedirnos hacer algo urgente.

Revisa la redacción

Muchas web y mensajes falsos tienen muchas faltas de ortografía en el texto.

Comprueba los enlaces

Pasa el ratón por encima del enlace para ver si pone lo mismo o lleva a otro sitio diferente.

Analiza los archivos adjuntos

Pasa el antivirus por los archivos.

Cómo descubrir páginas web falsas

Sigue estos consejos si no sabes si una web es falsa o no.

Revisa los enlaces

Revisa si son correctos y a dónde te llevan antes de pinchar.

Busca información sobre la empresa

Por ejemplo, la dirección de la empresa o el CIF de la empresa.
El CIF es un número que identifica a la empresa.
Es como su **DNI**.

DNI

Siglas de
Documento
Nacional de
Identidad

Busca información sobre la devolución de productos

Localiza si hay información sobre este tema.
En páginas falsas hay poca información o a veces ninguna.

Comprueba los precios y las descripciones de los productos

Sospecha si todos los precios son muy bajos o los artículos siempre están rebajados.
También sospecha si las descripciones no ayudan a comprar el producto.

Mira los comentarios y valoraciones de la tienda

Sospecha si solo hay comentarios positivos.
Lo normal es que una web tenga comentarios tanto positivos como negativos.

Revisa medios de pago

Fíate solo de aquellos comercios online que tienen opción de pago de tarjetas de crédito o Paypal.

8. Noticias falsas o bulos

Un bulo es una noticia falsa que se publica para hacer daño a alguien. Los bulos también se llama fake news. Fake news son palabras en inglés que significan noticias falsas.

Los objetivos de las noticias falsas son:

- **Desinformar.**
Si no estamos bien informadas es más fácil engañarnos.
- **Robo de información o introducir virus.**
Puede dañar nuestros dispositivos o robarnos información.
- **Dañar la reputación online.**
Puede dañar nuestros dispositivos o robarnos información.

Reputación online.

La imagen que tienen otras personas de ti a través de la información que hay en Internet.



Cómo detectar una noticia falsa

Busca la fuente.

Es decir, quién ha publicado la noticia de forma original o quién ha dicho qué..

Revisa el enlace.

Las noticias falsas se publican en páginas web falsas o poco fiables..

Atención al titular

Las noticias falsas tienen titulares muy sensacionalistas.

Comprueba el formato

Las noticias falsas no cuidan la presentación.

Usan imágenes de mala calidad o manipuladas y tienen faltas de ortografía.

Desconfía

si la intención de la noticia es dividir.

No te fíes

de imágenes o comentarios que llegan por Whatsapp y han sido reenviados muchas veces.



9. Otros fraudes

- **Anuncios maliciosos.**

Aparecen en medio de la pantalla
o en varios sitios
y buscan que pinches para llevarte
a una pantalla diferente.

- **Alquileres fraudulentos**

Están en las páginas web
de alquiler o compra de casas.
Suelen tener precios demasiado baratos.
Copian fotos de otros anuncios
las descripciones tienen poca información
o están mal escritas.
Cuando las personas llaman
ponen problemas para ir a visitar la vivienda.

- **Préstamos falsos**

Son anuncios en los que personas
anuncian dar préstamos por muy poco dinero.
El engaño es que tú pagas un poco de dinero
y luego la persona desaparece
y nunca te da ningún préstamo.

- **Concursos falsos**

Cuando te avisan de que has ganado
un concurso
sin haber participado nunca.
Usan formularios para conseguir tus datos.

- **Suscripciones por SMS**

Algunos servicios se financian
al cobrar dinero por cada SMS que enviamos.
Pero hay servicios que no te piden permiso
para hacerlo.

- **Sextorsion**

Cuando hay personas que nos piden contenido sexual para extorsionarnos o chantajearnos. Hay que tener cuidado y no acceder para evitar futuros problemas.



Seguridad en redes sociales

La identidad digital

Tu identidad digital es el conjunto de datos que se publican sobre ti en Internet.

Algunos de estos datos pueden ser:

- Imágenes
- Datos personales
- Comentarios
- Gustos
- Dónde has estado
- Quiénes son tus amigos

Es muy importante que sigas los consejos del siguiente punto.

10. Seguridad en redes sociales

Configura de forma segura tus perfiles en redes sociales

Tener seguridad en redes sociales es importante. Allí se comparte mucha información y es necesario que tengas el control sobre lo que compartes con el resto de las personas.

Aquí tienes algunas claves para hacerlo:

- Usa contraseñas fuertes.
- Activa la verificación en 2 pasos.
- Pon tu perfil privado.
Cualquiera puede acceder a tus datos y copiar o hacer capturas de pantalla de tus contenidos.
- Bloquea en tu perfil la opción de que personas que no conoces te envíen mensajes.
La mayor parte de los virus llega de personas desconocidas.
- Piensa antes de compartir.
Cuando pones una foto de tus vacaciones, amigos o aficiones estás dando demasiada información a gente desconocida.



- Cuidado con publicar comentarios agresivos o que ofendan a personas.
No escribas comentarios que no dirías cara a cara a la persona.
- Cierra tus sesiones cada vez que entres en ordenadores que no son solo tuyos.
- Si hay cosas publicadas sobre ti que tú no quieres, denúncialo.

Detecta una cuenta falsa

Las cuentas falsas son perfiles que se hacen pasar por otra gente. Estos perfiles se crean para engañar a otras personas y conseguir algo. Por ejemplo: dinero, datos o hacer chantaje a alguien. Todas las personas pueden ser víctimas de este engaño.

Una cuenta falsa también puede ser un perfil inventado que usa una mezcla de imágenes de usuarios.

¿Cómo puedes detectar que una cuenta es falsa?

- Usan fotos de mala calidad
- No hay casi descripción en sus perfiles.
- Tienen pocas publicaciones.
- Las publicaciones llevan a enlaces de web falsas que buscan conseguir información de las personas.
- Tienen pocos contactos.
- Tratan siempre el mismo tema.
Parece como si fuera un robot y no una persona.



¿Qué datos no debes compartir nunca?

- **Tu correo y número de teléfono.**

Si los compartes en tus redes personas desconocidas los pueden ver y pueden enviarte información o intentar engañarte.

- **Tu dirección o ubicación.**

La ubicación es dónde estás en este momento. No sabes qué pueden hacer otras personas con estos datos.

- **Fotos íntimas o sexuales.**

Hay personas que pueden usar estas fotos para hacerte chantaje.

- **Fotos de menores.**

No sabes dónde puede acabar esa foto. Tapa sus caras.

- **Documentos personales.**

Por ejemplo: tu DNI, dirección o datos bancarios. Personas pueden usar esos datos para hacerse pasar por ti.

- **Comentarios o quejas.**

Si haces comentarios demasiado agresivos puedes molestar u ofender a las personas.

- **Conversaciones privadas.**

No puedes compartir conversaciones con otra persona sin su permiso.

Reflexiona sobre este tema con este vídeo del INCIBE.
Escanea este código QR para verlo.



11. Usar Whatsapp de forma segura

Configura tu privacidad para controlar qué compartes y con quién.

Entra en el menú de whatsapp y pulsa **Ajustes > Cuenta > Privacidad**.

- Hora de última vez.

Para seleccionar quién ve cuándo te has conectado por última vez.

Puedes seleccionar que lo vea todo el mundo, solo tus contactos o nadie.

- Foto de perfil

Puedes seleccionar que lo vea todo el mundo, solo tus contactos o nadie.

- Info

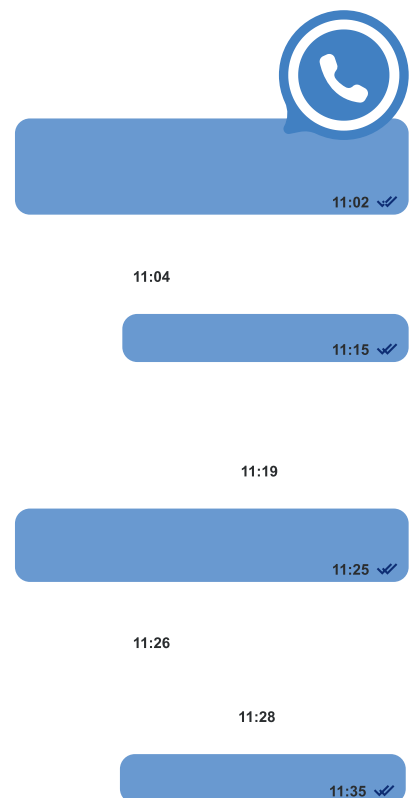
Puedes seleccionar que lo vea todo el mundo, solo tus contactos o nadie.

- Estado

Puedes seleccionar que los vean tus contactos, todos menos alguien o solo algunas personas.

- Confirmaciones de lectura

Significa que un contacto ha leído tu mensaje. Se representa por un tic azul. Puedes desactivarlo si quieres, pero entonces tú no verás si alguien ha leído tu mensaje.



- Grupos

Puedes seleccionar quién te puede agregar a los grupos.

- Ubicación en tiempo real

Aquí podemos ver si compartimos nuestra ubicación con algún contacto.

- Bloquear contactos

Puedes bloquear contactos en la aplicación. Pulsa en el icono de añadir contactos, selecciona el contacto que quieres bloquear. También puedes hacerlo desde la propia conversación con ese contacto.

- Activar el bloqueo con huella

Algunos móviles te dejan activar el bloqueo del móvil con tu huella.

Seguridad en compras y descargas

12. Compras online

Comprar online significa comprar un producto a través de Internet. Puedes comprar muchas cosas: desde ropa, comida o servicios. Por ejemplo: suscribirte a una plataforma para escuchar música.

Pero al igual que otras acciones en Internet, comprar de forma online tiene riesgos. Aquí tienes algunos consejos:

- Desconfía si hay productos con un precio demasiado bajo.
- Desconfía si la página te da poca información sobre el producto.
- Fíjate en las opiniones de otros usuarios. Si un producto no tiene opiniones o son muy malas, no lo compres.
- Comprueba si la página web es segura y empieza por “https://”
- Mira si las imágenes son de calidad y se ven bien.
- No te conectes en redes Wifi públicas para comprar de forma online.
- Desconfía si te pide demasiados datos que no son necesarios para la compra.
- Consulta tu cuenta bancaria después de la compra online.



13. Descargar programas y aplicaciones de forma segura

Descarga siempre las aplicaciones y programas en las páginas web oficiales. Así reducirás riesgos.

En el caso de los teléfonos móviles hay aplicaciones ya instaladas para descargar de forma segura.

- Play Store > Android
- App Store > iOS
- Microsoft Store > Microsoft

Estas aplicaciones son más seguras, pero no totalmente seguras.

Consejos para descargar aplicaciones:

- Mira el número de descargas de la aplicación.
- Mira los comentarios.
- Mira qué empresa ha creado la aplicación. y busca información sobre ella.
- Revisa qué permisos te pide la aplicación. Piensa para qué es la aplicación y que no es normal pedirte.



Hacer copias de seguridad

Copias de seguridad

Una copia de seguridad es una forma de proteger la información que guardas en tus dispositivos. Son copias de los archivos más importantes que se guardan en otro lugar.

Así si pierdes tu dispositivo, se daña o se infecta con un virus puedes recuperar esos archivos.



Puedes hacer las copias de 2 formas:

- De forma manual.
Eres tú quien te encargas de hacerlo.
- De forma automática.
Programas la copia para que el dispositivo lo haga solo.

Consejos:

- Haz copias cada poco tiempo y revisa que la copia esté bien hecha y guardada.
- No hagas copias de seguridad de todos tus archivos.
Haz las copias de los archivos que tengan más valor para ti: documentos importantes, fotos personales, correos con información importante y contactos.

Dónde guardar las copias de seguridad

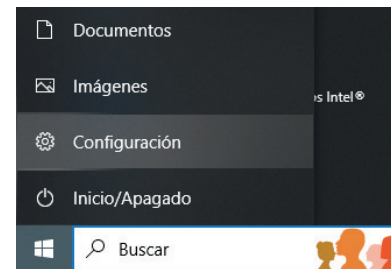
Puedes guardar las copias de seguridad en 2 lugares:

- En un servicio de la **nube**.
- En un disco duro externo.

Nube. Es un sitio de Internet que sirve para guardar archivos. Estos archivos no ocupan espacio en el ordenador y puedes acceder desde cualquier dispositivo.

Haz copia de seguridad en Windows

1. Haz clic en Inicio
y entra en configuración.



2. Entra en “actualización y seguridad”
y después pincha en “copia de seguridad”.
3. Pincha en “Agregar una copia de seguridad”
4. Elige donde quieres hacer la copia:
en un disco duro externo o en la nube.
5. Selecciona qué quieres guardar.
6. Da a “Iniciar copia de seguridad”.
7. Espera que termine.
8. Comprueba que la copia se ha hecho bien

Haz copia de seguridad en MacOS

La forma más fácil de hacer una copia de seguridad en el sistema MacOS es con la aplicación “Time Machine”.

1. Abre la aplicación “Time machine”
2. Elige donde quieres guardar la copia de seguridad
3. Después de la primera copia “Time Machine” hará copias a menudo de todos tus archivos.

Haz copia de seguridad en Android

Tienes que descargar la aplicación “Google One”.

1. Inicia sesión con tu cuenta de Google.
2. Selecciona los datos que quieres guardar.
3. Haz clic en el botón “Copia de seguridad” y después en “crear copia de seguridad ahora”.
4. Espera que termine.

Test final

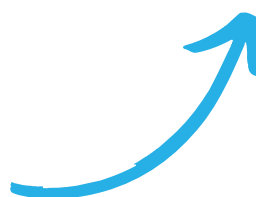


Test de evaluación

Escanea el código
y contesta a las preguntas



Para acceder al test
escanea el código con tu móvil



Diccionario

Actualizar un dispositivo. Descargar la última versión del sistema operativo.

Antivirus. Programa que protege nuestros dispositivos de virus y otras amenazas.

Baiting. USB infectado con virus en un sitio público para que una persona lo meta en su ordenador y puedan robar su información.

Beneficio. Mejora que una persona recibe. Por ejemplo: dinero.

Bluetooth. Es una tecnología para conectar dispositivos que están a poca distancia.

Bulo. Es una noticia falsa que se publica para hacer daño a alguien. Los bulos también se llama fake news.

Ciberseguridad. Proteger dispositivos y la información que hay en ellos de ataques informáticos.

Cookies. Son archivos que tu ordenador guarda cuando visitas una página web.

Copia de seguridad. Es una forma de proteger la información que guardas en tus dispositivos. Son copias de los archivos más importantes que se guardan en otro lugar.

Cuentas falsas. Son perfiles que se hacen pasar por otra gente. También pueden ser perfiles inventados.

Delincuentes. Personas que cometen un delito. Por ejemplo: robar

Dispositivo. Aparato informático que hace una tarea. Por ejemplo: un ordenador, un móvil o una tablet

DNI. Siglas de Documento Nacional de Identidad

Fraude. Un delito en el que una persona engaña a otra para conseguir un beneficio.

Historial. Es la lista de páginas web que has visitado.

Huella dactilar. Es la huella de los dedos. Identifica a una persona porque ninguna huella es igual a la otra.

Identidad digital. Es el conjunto de datos que se publican sobre ti en Internet.

Ingeniería social. Son las técnicas de engaño que usan los delincuentes para conseguir información.

Modo privado. El modo privado es una opción que puedes activar en tu navegador. Esta opción sirve para que tu navegador no guarde información como el historial, contraseñas, las cookies o la información de formularios. También se llama modo incógnito.

Nube. Es un sitio de Internet que sirve para guardar archivos. Estos archivos no ocupan espacio en el ordenador y puedes acceder desde cualquier dispositivo.

Pshishing. Son correos que se hacen pasar por alguien conocido o por una empresa para robar tus datos.

Reputación online. La imagen que tienen otros usuarios de ti a través de la información que hay en Internet.

Sextorsion. Cuando hay personas que nos piden contenido sexual para chantajearnos.

Smishing. Son mensajes de texto o SMS que se hacen pasar por empresas, bancos o personas conocidas para engañar a las personas y conseguir sus datos o controlar sus dispositivos.

Vishing. Son llamadas que se hacen pasar por empresas, bancos o servicios técnicos para engañar a las personas y conseguir sus datos o controlar sus dispositivos.



Paseo del Hospital Militar, 40, local 34
47006 Valladolid
983 320 116
www.plenainclusioncyl.org



Subvencionado por la Junta de Castilla y León con cargo a la asignación tributaria del IRPF



✓ POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL