

GUÍA MAESTRA DE CIBERSEGURIDAD

Protege tu *mundo digital*



vuela

A
Junta de Andalucía


Agencia Digital
de Andalucía

CONTRASEÑAS INFALIBLES

Tus contraseñas son la clave para acceder a tu vida digital, por eso es esencial que sean seguras y robustas.

Con **Andalucía Vuela**, aprende a transformar tus contraseñas en fortificaciones impenetrables para mantener tu información a salvo.

1. Usa un gestor de contraseñas



- Recordar decenas de contraseñas únicas y largas puede ser imposible.
- Aquí es donde los **gestores de contraseñas** se convierten en tus grandes aliados porque son **aplicaciones que almacenan** de forma segura todas tus claves en una "bóveda" cifrada, protegida por una única contraseña maestra.
- Así, solo tienes que recordar una y el gestor se encarga del resto, además de sugerirte claves robustas y únicas para cada servicio.

2. Usa una contraseña única para cada servicio y cámbiala de forma periódica



- Reutilizar la misma contraseña para diferentes plataformas es uno de los **mayores riesgos de seguridad**, ya que si un ciberdelincuente descubre tu clave de acceso en una filtración de datos, la probará en todos tus servicios: correo electrónico, redes sociales, banca, etc.
- Para evitar que eso pase, **usa una contraseña distinta** para cada cuenta y cámbiala de forma regular.

3. Activa la doble autenticación

- La **doble autenticación** es una capa extra de seguridad que añade un paso más a tu inicio de sesión.
- Además de tu contraseña, necesitarás un segundo factor, como un **código enviado a tu móvil** o, mejor aún, **generado por una app**. Este método hace que, aunque alguien descubra tu contraseña, no pueda acceder a tu cuenta sin tener tu dispositivo físico.



4. La longitud y la complejidad, claves de una contraseña segura

- Cuando tengas que recordar una contraseña, creala con al menos **12-16 caracteres** y que mezclen **números, mayúsculas, minúsculas y caracteres de puntuación y especiales**.
- Al **crear una contraseña segura**, no vale con escribir una palabra, números y algún símbolo, sino que hay que **integrar longitud y complejidad en una contraseña fácil de recordar para ti**.
- Un ejemplo de contraseña segura es una que incluya las **iniciales de una frase de tu canción favorita en mayúscula y minúscula**, varios caracteres y la fecha de nacimiento de una persona especial para ti.

Aprende más

Si quieres aprender más sobre contraseñas seguras, te recomendamos este curso gratuito de Aprende Volando:

Contraseñas seguras: protege tus cuentas y dispositivos

Modalidad: Online tutorizado y presencial - Duración: 10 horas

[Apúntate aquí](#)

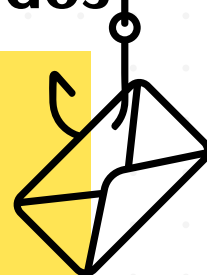
DETECTA EL PHISHING

El phishing es uno de los ciberataques más comunes, pero existe una serie de consejos y trucos para evitar que caigas en la trampa.

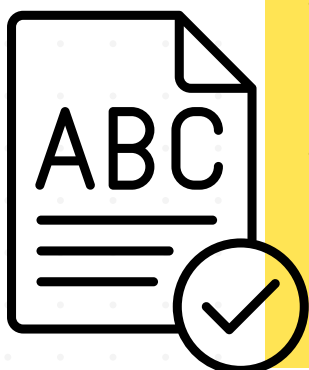
Con **Andalucía Vuela**, aprenderás a detectar el engaño y a defenderte.

1. Desconfía de remitentes desconocidos

- El primer paso es **siempre verificar quién te envía el mensaje**.
- Los ciberdelincuentes suelen **suplantar la identidad** de bancos, empresas de paquetería o servicios online conocidos.
- Si recibes un correo de alguien que no conoces o que te pide algo inesperado, **no hagas clic en ningún enlace ni descargues archivos**.
- La mayoría de las empresas jamás te pedirán datos personales por correo electrónico.
- Si tienes dudas con algún correo recibido, **contacta con quien creas que te envió el mensaje por otra vía de comunicación para confirmar**.



2. Cualquier tipo de mensaje puede ser una ciberestafa



- **Las empresas serias cuidan mucho su comunicación**. Si el mensaje **no parece profesional**, es una señal de alerta clara.
- Sin embargo, **el cibercrimen cada vez está más organizado y tiene mejores herramientas**, por lo tanto, aunque parezca un mensaje profesional, puede ser una **ciberestafa**.

3. Si algo parece demasiado bueno, quizá es porque es mentira

- Los estafadores utilizan **técnicas de manipulación** para que actúes de forma impulsiva con frases como *"tu cuenta será suspendida"*, *"acceso bloqueado"* o *"tienes una oferta por tiempo limitado"* que buscan **crear una sensación de pánico** y una respuesta emocional para que no pienses con claridad.
- Tómate un respiro, **verifica la fuente por un canal oficial** y nunca cedas a la presión. Recuerda actuar después de reflexionar.



4. Verifica los enlaces antes de hacer clic

- Antes de hacer clic en cualquier enlace, pasa el cursor sobre este y **observa la dirección web que aparece**, así como cuando se cargue, **comprueba la dirección**.
- Los estafadores usan direcciones que **imitan a las originales** (por ejemplo, *"https://juntadeandaluc1a.es"* en lugar de *"https://juntadeandalucia.es"*).
- Si la URL no es la oficial del servicio, no la abras. Siempre es mejor **teclea la dirección web en tu navegador directamente**.



Aprende más

Si quieres aprender más sobre un uso seguro del correo electrónico, te recomendamos este curso gratuito de Aprende Volando:

Uso seguro del correo electrónico

Modalidad: Online tutorizado - Duración: 10 horas

Apúntate aquí

DOBLE AUTENTICACIÓN

La doble autenticación es un paso adicional que multiplica tu seguridad. Te explicamos cómo funciona y por qué es fundamental activarla en todas tus cuentas.

Con **Andalucía Vuela** sube un escalón más en tu protección digital.

1. La autenticación de dos factores no es un extra, es un estándar



- Durante años, tu nombre de usuario y contraseña han sido la única barrera de seguridad. Pero **los ciberataques han evolucionado**, y las contraseñas pueden ser robadas o adivinadas.
- La **autenticación de dos factores** (2FA) o de múltiples factores (MFA) añade una segunda capa de seguridad. Es un paso extra que consiste en **demostrar de dos o más distintas formas que eres tú** a través de contraseñas, un mensaje que llega a tu teléfono personal o con la biometría.

2. Activa la doble autenticación en todas tus cuentas importantes

- No todos los servicios online ofrecen esta opción, pero es fundamental activarla en **aquellos que gestionan tu información más sensible**: correo electrónico, redes sociales, banca online y tiendas virtuales.
- Una vez que la actives, cada vez que intentes iniciar sesión, se te pedirá el segundo factor, independientemente de que sea un nuevo dispositivo o no.



3. Elige el método que más se adapte a ti



- Existen diferentes formas de autenticación de dos factores:
 - **Código por SMS:** el más popular y fácil de usar. Recibes un código numérico en tu teléfono móvil para confirmar el acceso. Puede ser vulnerable si alguien clona tu tarjeta SIM.
 - **Aplicaciones de autenticación:** son más seguras que los SMS y generan un código temporal que solo tú puedes ver.
 - **Llaves de seguridad físicas:** son dispositivos USB que se conectan a tu ordenador o móvil, por lo que son el método más seguro, ya que el ciberdelincuente necesitaría tener la llave física para poder acceder a tu cuenta.

4. No compartas el código de seguridad



- El código que recibes por SMS o en tu app de autenticación es **personal e intransferible**, pero los ciberdelincuentes a veces intentan engañarte para que les des este código.
- Recuerda: **las empresas legítimas nunca te pedirán este tipo de información**. Si recibes una llamada o un mensaje pidiéndote el código, cuelga o ignóralo. Es una trampa.
- Si recibes una petición de segundo factor y tú no has intentado iniciar sesión, deberías **cambiar tu contraseña y reportar a los responsables de la seguridad del sistema** que alguien podría haber tenido acceso a tus datos

Aprende más

Si quieres aprender más sobre sistemas de autenticación, te recomendamos este curso gratuito de Aprende Volando:

Tu "yo digital": identidad digital y sistemas de autenticación

Modalidad: Online tutorizado y presencial - Duración: 10 horas

[Apúntate aquí](#)

PRIVACIDAD EN REDES SOCIALES

Cada día compartimos información personal en redes sociales, pero, ¿quién puede ver realmente lo que publicas?

Con **Andalucía Vuela**, aprende a mantener tu vida privada en redes sociales bajo tu control, protegiendo tu información.

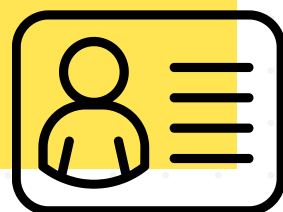
1. Configura tus perfiles como privados

- Esta es la **acción más importante para proteger tu privacidad**. De esta forma, solo las personas a las que has aceptado como seguidores o amigos podrán ver tus publicaciones. Así, evitas que desconocidos accedan a tus fotos, vídeos y comentarios.
- Revisa las **opciones de privacidad de cada red social** que utilices y asegúrate de que tus contenidos no estén visibles para todo el mundo.



2. Revisa las *apps* conectadas a tu perfil y no aceptes invitaciones desconocidas

- Es importante **revisar periódicamente las aplicaciones y juegos que acceden a tus cuentas**, eliminando las que no utilices. Esto **minimiza el riesgo** de que tus datos sean controlados sin consentimiento, previniendo robos de identidad. También deberías **revisar las condiciones de uso** de forma periódica para proteger tu privacidad.
- Aceptar **solicitudes de amistad** o seguimiento de perfiles que no conoces o que son sospechosos puede **poner en riesgo tu privacidad**.
- Estos perfiles pueden ser **cuentas falsas o bots** que buscan acceder a tu información personal para fines maliciosos, como el **robo de datos, el envío de spam o estafarte**.



3. Protege tu información personal



- **Evita compartir datos sensibles** como tu dirección, números de teléfono, detalles de tus vacaciones o información de tu trabajo.
- Cuanta menos información personal esté visible, **menor será el riesgo** de que sea usada para fines fraudulentos.

4. Sé consciente de tu huella digital



- Cada clic, cada "me gusta", cada comentario y cada publicación que haces deja un **rastro en Internet**: tu **huella digital**. Esta huella es un reflejo de tu identidad en línea, y puede ser usada para hacerse una idea de quién eres. La regla de oro es: si no lo dirías en voz alta en un lugar público, no lo publiques en redes sociales.
- Mantén una **huella digital positiva y profesional**, y haz limpieza periódica de publicaciones antiguas que ya no te representen así como de perfiles en redes sociales y aplicaciones que ya no uses.
- Te aconsejamos hacer **"ego surfing"** para ver qué se puede encontrar en Internet sobre ti así como acogerte a la **normativa de Protección de Datos Personales** para pedir a redes sociales y a otros servicios online que eliminen datos sobre ti que no quieres que estén en Internet.

Aprende más

Si quieres aprender más sobre privacidad en Internet, te recomendamos este curso gratuito de Aprende Volando:

Tu huella digital: controla y reduce tu rastro

Modalidad: Online tutorizado - Duración: 10 horas

Apúntate aquí

PROGRAMA ANTIVIRUS

En un mundo donde podemos encontrar diferentes amenazas digitales, desde virus hasta programas maliciosos, tu equipo necesita un escudo antivirus.

Con **Andalucía Vuela**, aprende a mantener tus equipos protegidos y seguros.

1. Elige un antivirus eficaz y de confianza



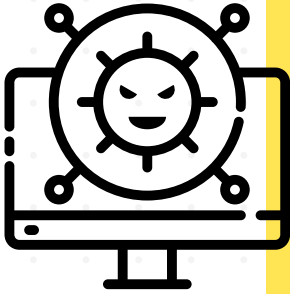
- Al elegir un antivirus **investiga sus características**: debe ofrecer protección en tiempo real contra la mayor variedad de tipos de amenazas posible como virus, troyanos, *ransomware* o *spyware*.
- Asegúrate de que detecta las amenazas tanto en los archivos que descargas como en tu navegación online.
- Es de gran importancia que las **actualizaciones sean constantes y automáticas**, para que te protejan de las amenazas más recientes.

2. Actualiza siempre tu software



- Los ciberdelincuentes explotan las **vulnerabilidades del software desactualizado**. Mantén siempre al día tu sistema operativo, así como tus aplicaciones y programas más usados, incluido el navegador web.
- Las **actualizaciones de seguridad** corrigen fallos que podrían ser aprovechados por los ciberdelincuentes para entrar en tu equipo.
- Por supuesto, estas medidas también se aplican a los **teléfonos móviles**, los grandes olvidados de la ciberseguridad.

3. Haz análisis periódicos de tu equipo



- Además de la protección en tiempo real, es recomendable hacer **análisis de tu equipo de forma regular**. Programa un escaneo completo de tu sistema al menos una vez a la semana.
- Un **análisis en profundidad** puede detectar amenazas que hayan podido pasar desapercibidas y eliminarlas antes de que causen daños.

4. Utiliza el sentido común en tu navegación y en tu correo electrónico



- Aunque tengas un antivirus, **debes seguir teniendo cuidado. Sin ti, no hay seguridad**. Complementa la protección de tu software con **hábitos de navegación seguros**:
 - Evita visitar sitios web sospechosos o con publicidad intrusiva.
 - No descargues archivos de fuentes no oficiales o piratas.
 - Nunca abras un enlace o adjunto de un correo electrónico que no esperabas.
 - Revisa el remitente de los correos y no hagas clic en enlaces ni ficheros adjuntos.
- Recuerda: Una adecuada prevención es imprescindible para mantener tu equipo seguro.

Aprende más

Si quieres aprender más sobre proteger tus dispositivos, te recomendamos este curso gratuito de Aprende Volando:

Protégete contra el malware

Modalidad: Online tutorizado - Duración: 10 horas

Apúntate aquí

COPIAS DE SEGURIDAD

Por un fallo técnico, un ciberataque o un simple error humano puedes perder para siempre tus recuerdos y documentos más valiosos.

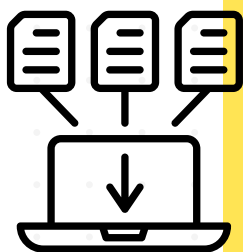
Con **Andalucía Vuela** aprende a proteger la información que más te importa.

1. La regla 3-2-1: tu mejor estrategia de seguridad

- Una copia de seguridad sirve para si sufres un robo, un incendio o una inundación, tus archivos más importantes siempre estén a salvo en otra ubicación.
- La clave para una buena copia de seguridad es **no dejar nada al azar**.
- La **regla 3-2-1** es tu guía: ten al menos **3 copias de tus datos**, guárdalas en **2 tipos de medios diferentes** (por ejemplo, en un disco duro externo y en la nube) y deja **1 de esas copias fuera de casa** o de tu lugar de trabajo.

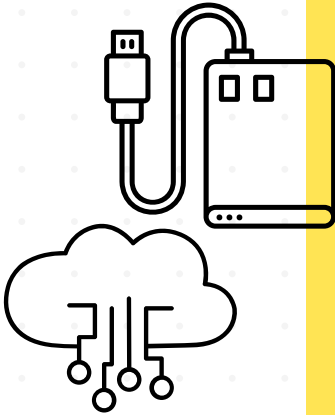


2. Automatiza tus copias de seguridad



- No programar las copias de seguridad para que se hagan de forma automática es un error, ya que es fácil que se nos olvide o que lo dejemos para otro día.
- Configura tu sistema operativo o usa programas específicos para que las **copias se hagan de forma automática y programada**.
- Puedes programarlas para que se ejecuten una vez a la semana o incluso de forma diaria, según la frecuencia con la que trabajes con tus archivos.

3. No confíes en un solo tipo de soporte



- Tener todos tus archivos en un solo disco duro o en la nube puede parecer práctico, pero **es un riesgo si alguno falla**. Lo más seguro es **combinar diferentes soportes**.
- Usa un disco duro externo, un servicio de almacenamiento en la nube o incluso una memoria USB para tener tus archivos duplicados y seguros en todo momento.

4. Guarda tus copias de seguridad en un lugar seguro



- Una vez que has creado tus copias de seguridad, es crucial que las protejas.
 - Si usas un **disco duro externo, un pendrive o una tarjeta de memoria**, guárdalos en un lugar seguro para evitar que se dañe o se pierda.
 - Si utilizas un **servicio en la nube**, asegúrate de que esté protegido con una contraseña robusta y con la doble autenticación.
- Tus **copias de seguridad son tan valiosas** como tus archivos originales, ¡trátalas como tal!

Aprende más

Si quieres aprender más sobre copias de seguridad, te recomendamos este curso gratuito de Aprende Volando:

Organiza tus archivos en la nube

Modalidad: Online tutorizado y presencial - Duración: 10 horas

Apúntate aquí

EL CERTIFICADO DIGITAL

En el mundo físico, usas tu DNI para identificarte. En el mundo online, tu identidad se verifica con un certificado digital.

Con **Andalucía Vuela** aprende a proteger tu identidad en Internet

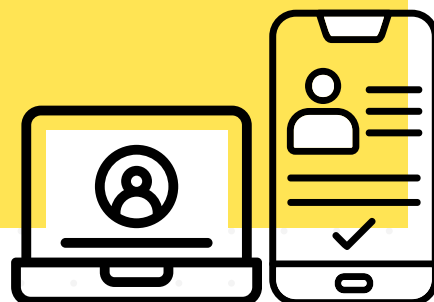
1. El certificado digital es tu DNI en el mundo online



- Es una **herramienta** que te permite identificarte en Internet de forma segura, a modo de **firma digital** que garantiza tu identidad y la integridad de tus comunicaciones.
- Es esencial para **realizar trámites** con la Administración Pública, como firmar documentos oficiales, consultar tu vida laboral o pedir cita médica.

2. Úsalo con cuidado y solo en equipos de confianza

- El certificado digital es una herramienta poderosa que te **da acceso a tu información más sensible**. Por ello, es crucial usarlo solo en **equipos personales de confianza**, ya sea tu portátil o tu teléfono móvil.
- Evita instalarlo en ordenadores públicos o de uso compartido, ya que **podría ser copiado y utilizado por ciberdelincuentes para usurpar tu identidad** y realizar trámites en tu nombre.
- También el **certificado debe tener una contraseña** para impedir que otras personas utilicen tu identidad.



3. Revoca tu certificado en caso de robo o pérdida

- Si tu portátil, tableta o móvil con el certificado instalado se pierde o tienes sospechas de que alguien podría habértelo robado, actúa de inmediato. Debes **revocar tu certificado digital** para anularlo y evitar que alguien lo utilice para realizar trámites en tu nombre.
- Contacta o visita la web de la **entidad emisora del certificado** (la Fábrica Nacional de Moneda y Timbre, la Policía Nacional...) para iniciar el proceso de revocación lo antes posible.



4. Confirma el tiempo de validez de tu certificado

- Los **certificados digitales no duran para siempre**. Tienen un periodo de validez, pasado el cual, caducan.
- Revisa de forma periódica el **tiempo restante de tu certificado** para que puedas renovarlo dentro del plazo. Así, evitarás interrupciones en tus trámites online.
- Recuerda **borrar tu certificado caducado** de cualquier dispositivo para evitar el acceso a tu información personal.



Aprende más

Si quieres aprender más sobre certificados electrónicos, te recomendamos este curso gratuito de Aprende Volando:

Certificado electrónico. Cómo obtenerlo y dónde utilizarlo

Modalidad: Online tutorizado y presencial - Duración: 10 horas

Apúntate aquí

Checklist definitivo de ciberseguridad

Accesos y contraseñas

- ☐ ¿Utilizas una contraseña distinta y única para cada uno de tus servicios?
- ☐ ¿Tus claves tienen una longitud de entre 12 y 16 caracteres e incluyen números, símbolos y letras?
- ☐ ¿Gestionas tus claves con un gestor de contraseñas para no tener que recordarlas todas?
- ☐ ¿Has activado la doble autenticación (2FA) en tus cuentas?

Protección de tus dispositivos

- ☐ ¿Tienes instalado un programa antivirus que ofrezca protección en tiempo real?
- ☐ ¿Mantienes el sistema operativo, el navegador y todas tus aplicaciones siempre actualizados?
- ☐ ¿Proteges también tu teléfono móvil con las mismas medidas de seguridad que tu ordenador?

¡No caigas en estafas!

- ☐ ¿Verificas la identidad del remitente antes de contestar?
- ☐ ¿Pasas el cursor sobre los enlaces para comprobar la URL real antes de hacer clic?
- ☐ ¿Evitas descargar archivos de fuentes que no son oficiales o que te generan dudas?

Checklist definitivo de ciberseguridad

Privacidad y redes sociales

- ☐ ¿Has configurado tus perfiles como privados para que solo tus amigos vean lo que publicas?
- ☐ ¿Revisas y eliminas periódicamente las aplicaciones o juegos conectados a tus perfiles que ya no usas?
- ☐ ¿Evitas compartir datos sensibles como tu dirección particular, detalles del trabajo o tus vacaciones?

Certificado digital

- ☐ ¿Utilizas tu certificado digital exclusivamente en equipos personales de confianza?
- ☐ ¿Le has asignado una contraseña propia para evitar que otros suplanten tu identidad?
- ☐ ¿Revisas periódicamente la fecha de validez para renovarlo antes de que caduque?

Copias de seguridad

- ☐ ¿Sigues la regla 3-2-1 (3 copias, 2 soportes distintos y 1 fuera de tu ubicación habitual)?
- ☐ ¿Tienes programadas tus copias de seguridad para que se realicen de forma automática?
- ☐ ¿Proteges tus copias en la nube con una contraseña robusta y doble autenticación?

vuela

Más cerca, más digitales, más oportunidades

andaluciavuela.es

