

1. IDENTIDAD DIGITAL Y SEGURIDAD



S!LBO

Tu Ayuda Digital

INICIO

Todas tus actuaciones dentro del espacio digital (imágenes, comentarios, enlaces visitados, lugares donde publicamos tus datos, etc.) conforman nuestra identidad o perfil digital. Una de las competencias personales necesarias para el ciudadano digital es el saber gestionar su propia identidad digital, actuando de una manera ética y legal dentro de una correcta cultura de la participación.

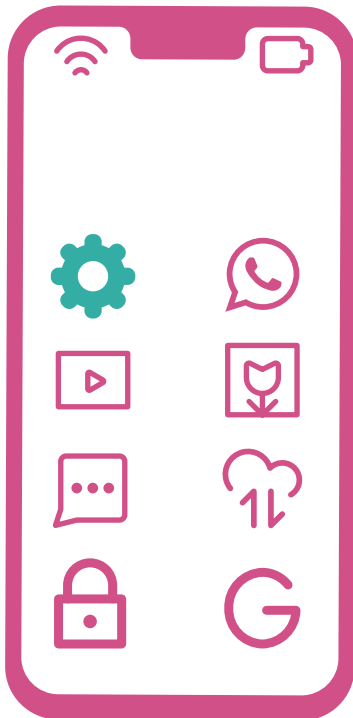
Gestión de la identidad digital

Hay dos formas de ver la identidad digital e Internet. Una es creer que la presencia virtual significa un peligro para la seguridad personal. La otra perspectiva es entender la construcción de la identidad en la red como una oportunidad de aprendizaje dentro de la cultura informacional donde vivimos inmersos.

En este manual aprenderemos cómo comunicar con tu dispositivo, no paso a paso como un tutorial, sino entendiendo los términos, funciones y lógicas de las diferentes empresas que nos dan servicios dentro y fuera de nuestros entornos digitales.

Tu dispositivo es algo así como un centro comercial donde interactúan muchas empresas que gestionan su funcionamiento.

Puedes decidir en qué “empresas” entras pero ellas siempre van a decidir muchas cosas por ti. Tenlo en cuenta.



Rellena este formulario con los datos de tus dispositivos portátiles. Si no conoces alguna de las cuestiones, no te preocupes, déjalo en blanco.

Marca y modelo

Android **Apple**

Compañía telefonía

Versión

Correo electrónico para la descarga de APPs

Marca y modelo

Android **Apple**

Compañía telefonía

Versión

Correo electrónico para la descarga de APPs

Si tienes un dispositivo portátil conectado a Internet (teléfono, tablet o reloj), tienes tres elementos de seguridad que entran en juego.

- ✓ El desbloqueo de tu dispositivo.
- ✓ El PIN! de la tarjeta SIM! (tu conexión de datos y telefonía).
- ✓ Un correo electrónico asociado al dispositivo.

Estos elementos están asociados a las tres empresas que te dan servicio. La empresa de telefonía, la empresa fabricante del dispositivo y la empresa propietaria del sistema operativo.



GESTIÓN DE CONTRASEÑAS SEGURAS

Tipos de contraseñas



Contraseñas numéricas de 4 o 6 cifras. Suelen ser para acceder a la SIM o acceso rápido al dispositivo. O las de tu tarjeta del banco para utilizar en cajeros automáticos. También se llama PIN.



El patrón de desbloqueo. Es una medida de seguridad básica y se está tendiendo a no utilizar.

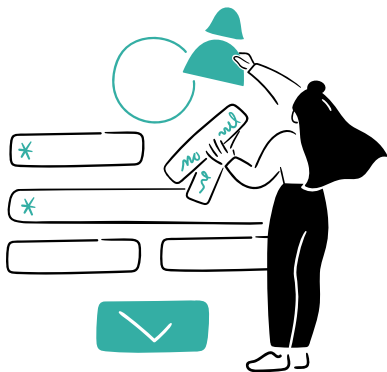


Contraseñas alfanuméricas. Contraseñas complejas para acceder a servicios. Cada compañía tiene sus reglas.



Contraseñas biométricas. Puede ser tu cara o tu huella y lo gestiona tu dispositivo.

¡OJO!, si te acostumbras a utilizar tu huella, puedes olvidar tus contraseñas.



¿Cómo hacer una contraseña y recordarla?

Mezclar letras, números, minúsculas, mayúsculas y símbolos también es algo casi obligatorio si se quiere una clave fuerte. Con estos tres elementos, hay varios trucos para recordar contraseñas que cumplan con estos requisitos.

Frase como contraseña. Nada como coger algo memorable sobre ti, algo que sepas de memoria desde hace décadas, y mezclarlo de una forma que vas a recordar, incluso si al principio cuesta un poco.

PAO. Persona, acción y objeto. Puedes utilizar palabras que no estén relacionadas entre sí. Cuidado con usar nombres de películas o citas célebres.

Lo importante, casi tanto como que la contraseña sea segura, es recordarla al instante.

Requisitos de acceso con doble factor. Una medida de seguridad extra que algunas empresas están comenzado a utilizar es que nos notifican por otro dispositivo para confirmar un pago o una transacción económica.

CONOCE TUS DISPOSITIVOS

Lo primero es identificar tus diferentes dispositivos, proveedores y cómo te conectas a ellos. Uno te da la **conectividad** y otro te da el acceso al teléfono y sus aplicaciones (**Apps**).

- ✓ Proveedor de servicios de Internet (**ISP**)!
Operador de telefonía.
- ✓ Propietario del sistema operativo del dispositivo. Puede ser con una cuenta de **Google (Android)**! o de una cuenta de **Apple**! depende del sistema operativo (**OS**) que dispongas. Esto no depende de tu operador (el que manda las facturas del gasto telefónico y datos).



Las empresas de telefonía puede ofrecer servicios distintos al de internet, como televisión. Incluso venderte el dispositivo o venderte una suscripción mensual de música, series o películas.

HBO **Netflix** **Filmin** **Spotify** ...

¿Dónde y cómo te conectas?

Hay que saber distinguir si te conectas con datos (**3G**, **4G** o **5G**)! o con una **Wifi**, ya sea la de casa o de confianza o una **Wifi** en la calle o en un local privado o pública (cafetería, aeropuerto, etc). Ten en cuenta que algunas conexiones **Wifi**! tienen limitaciones de tiempo y uso.

Otras conexiones pueden ser para unir otros dispositivos como auriculares, manos libres, bafles (**Bluetooth**)! o para hacer pagos (**NFC**)!

Normalmente todas estas conexiones se gestionan desde un acceso directo de la pantalla del dispositivo donde podrás encontrar estos iconos junto con el nombre de la compañía telefónica.



4G



NFC

¿Qué es lo que tengo instalado en mi dispositivo?

En tu dispositivo siempre tienes un sistema operativo para gestionar todo lo necesario, que contiene diferentes aplicaciones (**APPS**)! que te permiten diferentes usos, es como el engranaje de una navaja suiza.

Hay aplicaciones (**APPS**) para gestionar los propios dispositivos preestablecidas por nuestro sistema operativo y no se pueden borrar. Son como las tripas de aparato.



El teléfono que el gobierno pone a tu disposición **017** centraliza los servicios de atención telefónica relativos a dudas o consultas sobre ciberseguridad, privacidad y confianza digital.



¿Qué tengo que saber al instalar una aplicación en mis dispositivos?

Hay APPs de funcionalidades variadas de terceras compañías que nos pueden ayudar a guardar información, medir, fotografiar, etc... Estas se pueden instalar mediante lo que se denominan “Mercados de Apps”: **Google Play!** o **App Store!** Pueden ser gratuitas, de pago o de suscripción por uso.





- ✓ Verifica que la **App** es compatible con tu sistema operativo.
- ✓ Revisa con atención qué información te está solicitando la App.
- ✓ Lee reseñas y comentarios de [nuestr@s](#) voluntari@s.



TUS DATOS

¿Dónde están mis datos?

Los datos están almacenados en el dispositivo, de forma interna, mediante una tarjeta de memoria o en la nube de almacenamiento de tu proveedor. Para acceder a ellos normalmente tendrás que teclear la contraseña de tu dispositivo gestionado por el sistema operativo.

No la confundas con la contraseña de tu **SIM**,  ! puede ser diferente. ¡Ojo!, si la bloqueas, tendrás que acceder al **PUK**.  !

El espacio extra de memoria en el dispositivo suele ser una tarjeta de memoria **microSD**.!



Copia de seguridad!



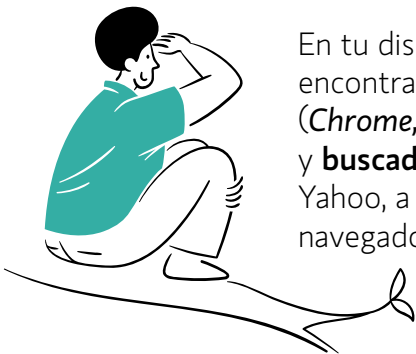
El almacenamiento en la nube es un modelo de servicio en el cual los datos se almacenan, se administran y se respaldan de forma remota, en servidores que están y son administrados por un proveedor del servicio que contratamos o nos regalan.

Con este servicio accesible vía internet desde cualquier lugar, podemos hacer uso de la sincronización de nuestros datos, (agenda, calendario, fotos) incluso una copia de seguridad para nuestros dispositivos.



Si haces una copia de seguridad podrás utilizar esa información en caso de que cambies el dispositivo, lo pierdas o se estropee.

TUS DATOS



En tu dispositivo siempre encontrarás un **Navegador!** (*Chrome, Firefox o Safari...*) y **buscadores!** como Google, Yahoo, a veces integrados en los navegadores.

Gestión de notificaciones y permisos de uso.

Cuando instalas una App de un tercero debes decidir qué permiso decides darle para obtener tu ubicación (**GPS!**), cámara, datos almacenamiento, sensores, contactos, micrófono, teléfono y **SMS!**


Debes leer atentamente los mensajes, ya que si no das permisos para algunas de sus peticiones, la aplicación no funcionará correctamente. Si crees que no es necesario darle permisos para notificarte avisos, no lo hagas. Tú decides hasta dónde quieres llegar.


Hay veces que no puedes instalar una aplicación porque tu sistema operativo es antiguo o no tienes espacio. Toca hacer limpieza, o decidir comprar un nuevo dispositivo.

Sincronización.

Si quieres tener tus datos sincronizados, estos estarán vinculados a una cuenta de correo electrónico (normalmente de Google o Apple).







Borrado remoto. Es una función de seguridad para gestionar dispositivos móviles que te permite borrar datos a distancia de dispositivos que hayas perdido o te hayan robado.

Actualizaciones de seguridad. Es conveniente actualizar nuestro dispositivo de forma regular, con eso conseguiremos estar más protegidos.

- ! Existe un diccionario en papel y en línea que explica las palabras o frases marcadas.

MANUALES S!LBO



1. Identidad digital y seguridad
2. Administración electrónica
3. Comercio y dinero electrónico
4. Información digital
5. Socialización digital



Fundación
PEM

En colaboración con:



UNATE

—La Universidad Permanente—

ENTIDAD DECLARADA
DE UTILIDAD PÚBLICA

Con el apoyo:



tuayudadigital.net