Bloqueo de dispositivos: ¿por qué es importante?

Hoy en día todos los teléfonos móviles, tablets y ordenadores disponen de algún mecanismo para evitar que cualquier usuario pueda hacer uso de nuestro dispositivo, ya sea una contraseña, un PIN o incluso una huella dactilar. Si alguna vez nos hemos preguntado cómo funcionan estas medidas de protección, en este artículo veremos todas ellas, de qué nos protegen y por qué son tan importantes para nuestra seguridad y la de nuestros dispositivos.

Todos nuestros dispositivos contienen una cantidad enorme de información personal, como mensajes, fotografías y vídeos que vamos almacenando; datos de nuestros contactos; correos con contactos y documentos privados, etc., y para protegerlos nos servimos de una gran variedad de herramientas de seguridad. Una de las primeras configuraciones de seguridad que realizamos cuando encendemos por primera vez nuestro equipo es el **bloqueo de acceso**, ya sea mediante un PIN, un patrón o una clave de seguridad.

Del mismo modo que protegemos nuestro hogar con una cerradura y su llave, o nuestros bienes más preciados dentro de una caja fuerte con una contraseña, la función del bloqueo de acceso es impedir que otra persona pueda utilizar nuestro dispositivo y acceder a la información almacenada en ellos. Imaginemos que nuestro hogar estuviera abierto de par en par, cualquiera podría entrar y acceder a nuestros bienes personales o incluso robarlos.

El bloqueo de nuestros dispositivos es fundamental para nuestra seguridad. A continuación, vamos a hacer un repaso sobre los métodos de bloqueo presentes en los diferentes sistemas operativos:

Bloqueo de dispositivos móviles

Nuestros dispositivos móviles (*smartphones o tablets*) cada vez son más necesarios en nuestro día a día, ya que los utilizamos para realizar llamadas y videollamadas con nuestros familiares y amigos, almacenar fotografías, navegar por Internet y realizar compras.

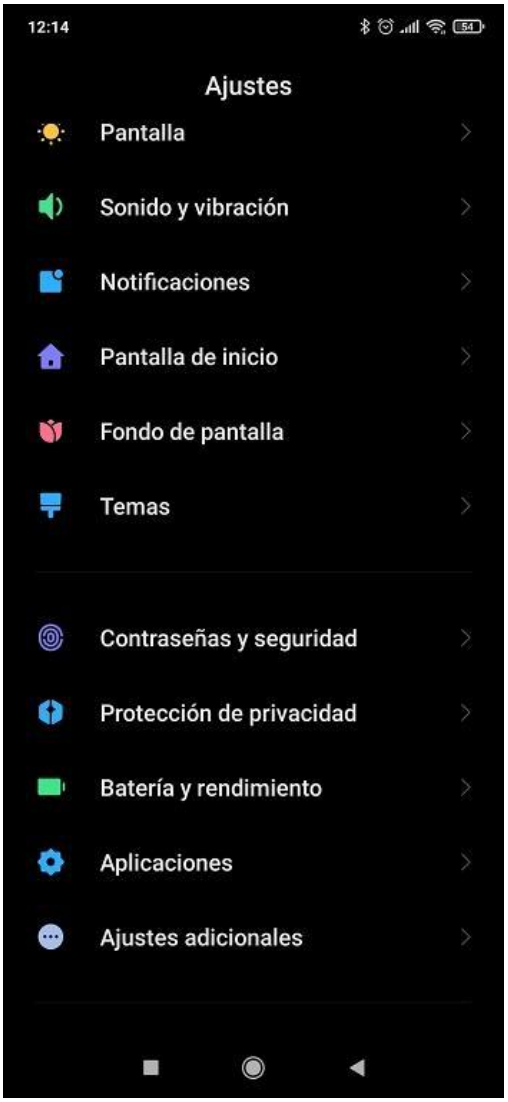
Para protegerlos contamos con una herramienta muy importante que es el sistema de bloqueo de nuestros dispositivos. Veamos cómo funciona paso a paso:

Dispositivos Android: android

Android es un sistema operativo que podemos encontrar en una gran variedad de dispositivos móviles, como *tablets o smartphones*. Si no conocemos cuál es el sistema operativo de nuestro dispositivo, al encender y apagar el dispositivo podemos fijarnos en el nombre del sistema que aparece y en su icono.

Para configurar el **bloqueo de pantalla** en nuestros dispositivos Android deberemos seguir los siguientes pasos, aunque pueden variar dependiendo de nuestra versión de Android y el modelo de nuestro *smartphone* (en este caso utilizaremos un dispositivo Xiaomi):

Abriremos la aplicación **'Ajustes'** (icono de una rueda dentada), que podemos encontrar en el escritorio o en la pantalla de menú, y seleccionaremos la opción **'Contraseña y seguridad'**. Buscaremos la sección de 'Seguridad' y, a continuación, **'Bloqueo de pantalla'**.



1. Si pulsamos sobre **'Contraseñas'**, accederemos a los diferentes tipos de bloqueo de pantalla:

- **Patrón**: consiste en un dibujo trazado uniendo una serie de nueve puntos en forma de un cuadrado de 3x3. Es la opción menos segura, ya que cualquiera puede ver el trazo en la pantalla.

- **PIN**: se trata de una clave de al menos 4 dígitos. Te recomendamos no utilizar el mismo PIN de la tarjeta SIM o la del banco.
- **Contraseña**: se trata de una clave de al menos 4 dígitos y letras. Debemos utilizar una contraseña difícil de averiguar y única para el dispositivo.

2. Las otras opciones son:
   - **Desbloqueo con huella dactilar**: nuestro dispositivo dispone de un lector de huella dactilar. Puede utilizarse para que una o varias huellas dactilares desbloqueen nuestro móvil o *tablet* simplemente poniendo el dedo sobre el lector de la huella.
   - **Desbloqueo facial**: nuestro dispositivo es capaz de reconocer rostros mediante la cámara frontal. Podemos añadir nuestro rostro o el de otros usuarios como mecanismo de desbloqueo.
   - **Desbloquear con dispositivo Bluetooth**: podremos utilizar otro dispositivo inteligente para desbloquear nuestro móvil o *tablet*, como una pulsera de actividad o reloj inteligente.

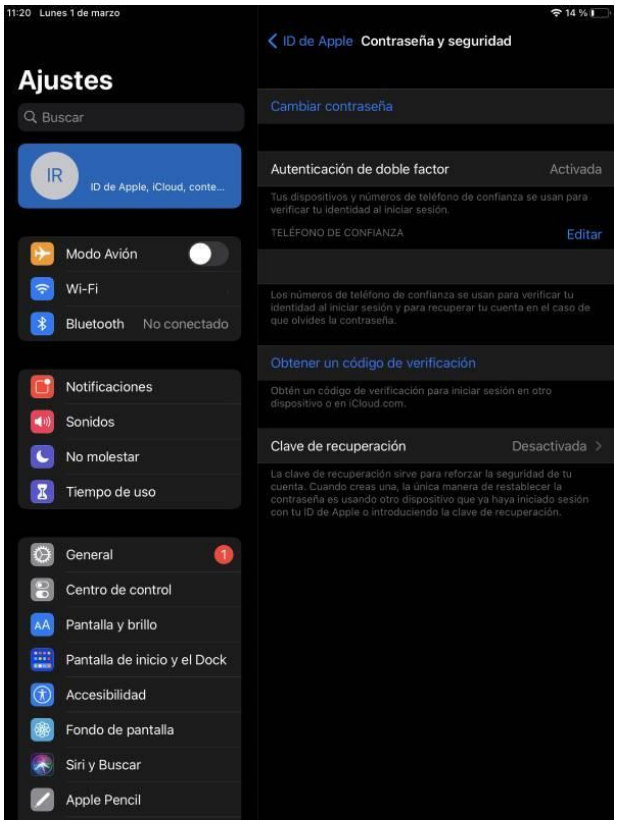
Cuando hayamos escogido la opción deseada, preferiblemente las últimas opciones, deberemos **seguir los pasos** para configurarla e implementarla como mecanismo de desbloqueo. Nuestro dispositivo nos solicitará que configuremos más de un método de desbloqueo para poder utilizarlo en el caso de que el primero falle y como medida de seguridad extra.

Dispositivos iOS

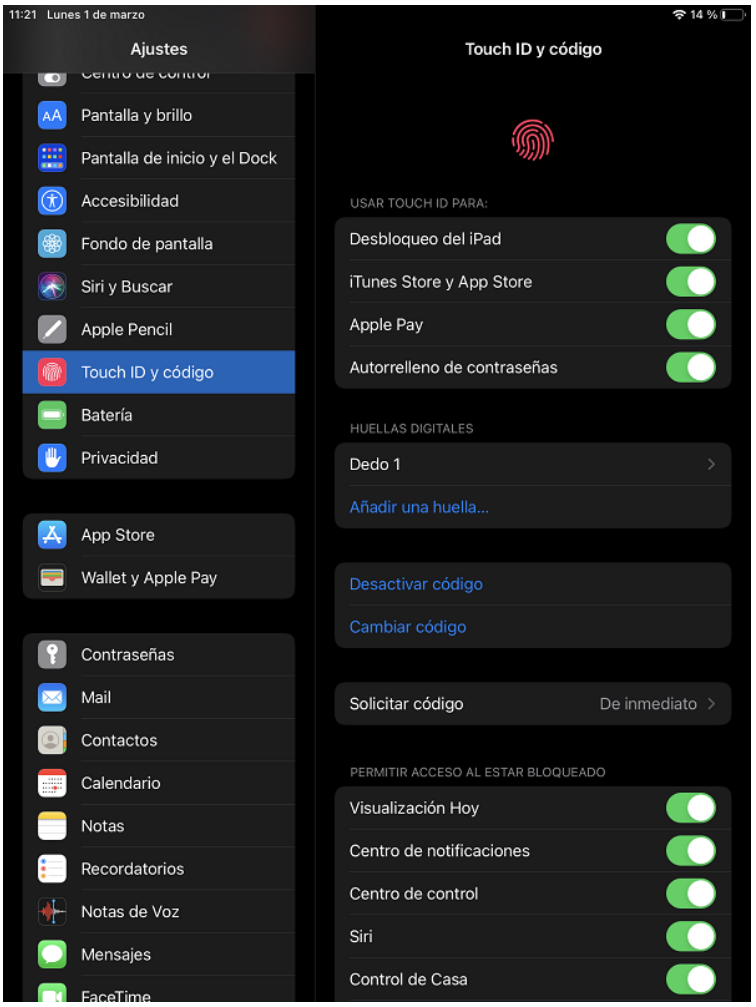
Cuando adquirimos un dispositivo de la marca Apple (con el icono de una manzana), como un iPhone (teléfono) o un iPad (*tablet*), nos pedirá establecer un código de 8 cifras para desbloquearlo la primera vez que lo encendamos. Este código será la clave que necesitaremos para desbloquearlo cada vez que lo encendamos a partir de ahora.

En algunos modelos es posible utilizar nuestra **huella dactilar** o incluso el reconocimiento de nuestro **rostro** para proteger nuestro dispositivo. Podemos configurar estas medidas de bloqueo/desbloqueo siguiendo estos pasos:

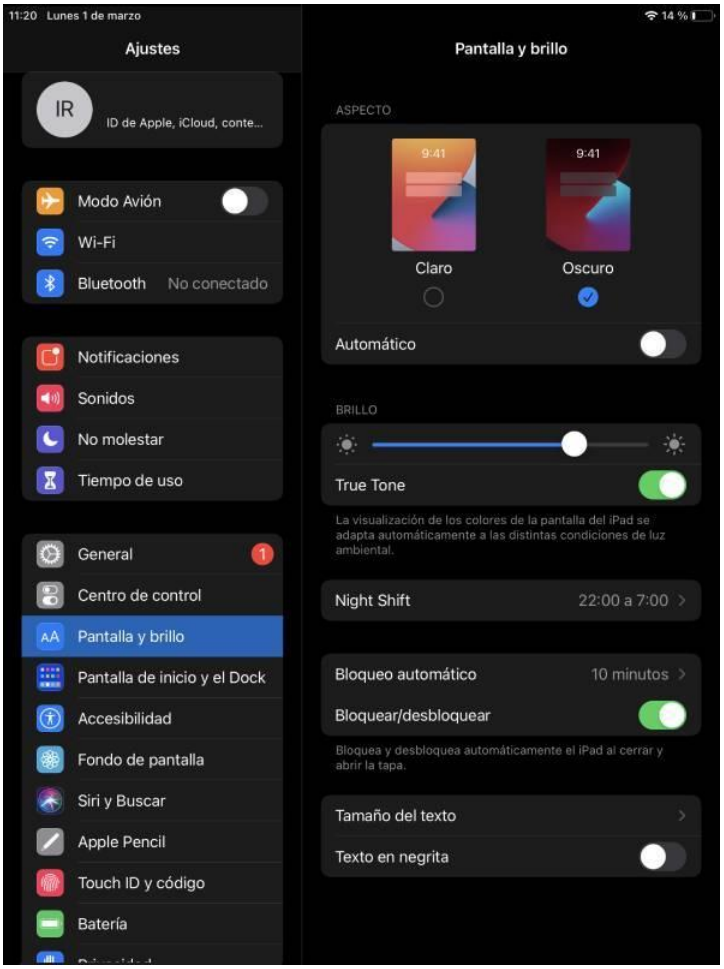
1. Accederemos a **'Ajustes'** (icono de una rueda dentada), que podemos encontrar en el escritorio, y seleccionamos **ID de Apple > Contraseña y seguridad > Cambiar contraseña**. Desde aquí podremos cambiar la clave a una más robusta, estableciéndola como mínimo de 8 caracteres, incluyendo al menos una mayúscula, una minúscula y un número; por ejemplo: MiIph0ne11.



2. Dentro de **'Ajustes'** buscaremos las opciones **Touch ID** o **Face ID** (en los modelos más nuevos). Dentro podremos:
    - Activar el desbloqueo del iPad/iPhone.
    - Añadir una nueva huella o nuestro rostro con alguna modificación.
    - Solicitar el código (contraseña) como medida de seguridad adicional.



3. También podremos configurar el tiempo que el dispositivo estará inactivo antes de activarse el bloqueo automático. Para ello, iremos a **Ajustes > Pantalla y brillo**, donde encontraremos la opción de **'Bloqueo automático'**.


11:20 Lunes 1 de marzo
14 %
Ajustes
IR
ID de Apple, iCloud, conte...
Modo Avión
Wi-Fi
Bluetooth
No conectado
Notificaciones
Sonidos
No molestar
Tiempo de uso
General
Centro de control
Pantalla y brillo
Pantalla de inicio y el Dock
Accesibilidad
Fondo de pantalla
Siri y Buscar
Apple Pencil
Touch ID y código
Batería
Pantalla y brillo
ASPECTO
9:41
9:41
Claro
Oscuro
Automático
BRILLO
True Tone
La visualización de los colores de la pantalla del iPad se adapta automáticamente a las distintas condiciones de luz ambiental.
Night Shift
22:00 a 7:00
Bloqueo automático
10 minutos
Bloquear/desbloquear
Bloquea y desbloquea automáticamente el iPad al cerrar y abrir la tapa.
Tamaño del texto
Texto en negrita

Bloqueo de ordenadores

Nuestros ordenadores, como nuestros dispositivos móviles, también contienen mucha información que debemos proteger. Para poder hacerlo cuentan con diferentes mecanismos, como medidas de bloqueo o cuentas de usuario con distintos privilegios.

Cuando hablamos de **cuentas de usuarios y sus privilegios** podemos imaginarnos una ciudad, donde el **administrador** sería el alcalde, que se encarga de dirigir la ciudad, aplicar leyes y gestionar sus recursos, mientras que los **usuarios** seríamos los habitantes de la ciudad que hacen uso de todos sus servicios, teniendo capacidad de toma de decisiones solo dentro de nuestro propio hogar, por ejemplo, para modificar el termostato, elegir los muebles, etc.

Por ello mismo, cuando hablamos de tipos de cuentas de usuario lo más seguro es utilizar una sola cuenta de administrador y una contraseña robusta, tanto para dicha cuenta como para el resto de cuentas de usuarios.

Ordenadores Windows

En los ordenadores o portátiles con el sistema operativo de Microsoft Windows podemos crear varias cuentas de usuario para que todos los miembros de la casa puedan utilizar un mismo equipo:

1. En Windows existen principalmente dos tipos de cuentas: **las cuentas de administrador, que son capaces de realizar modificaciones dentro del sistema, y las cuentas de usuario, que son las afectadas por las modificaciones del sistema.**
2. La posibilidad de crear múltiples cuentas implica que cada usuario tenga la suya. Si estas cuentas no están debidamente protegidas, **cualquier usuario podría acceder a la información personal del resto.**

Para evitar este tipo de situaciones lo más seguro es crear **una única cuenta de administrador y proteger el acceso al resto de cuentas** correctamente, aplicando un bloqueo de acceso o pantalla. Por defecto, cuando se crea una cuenta en Windows 10 hay que incluir:

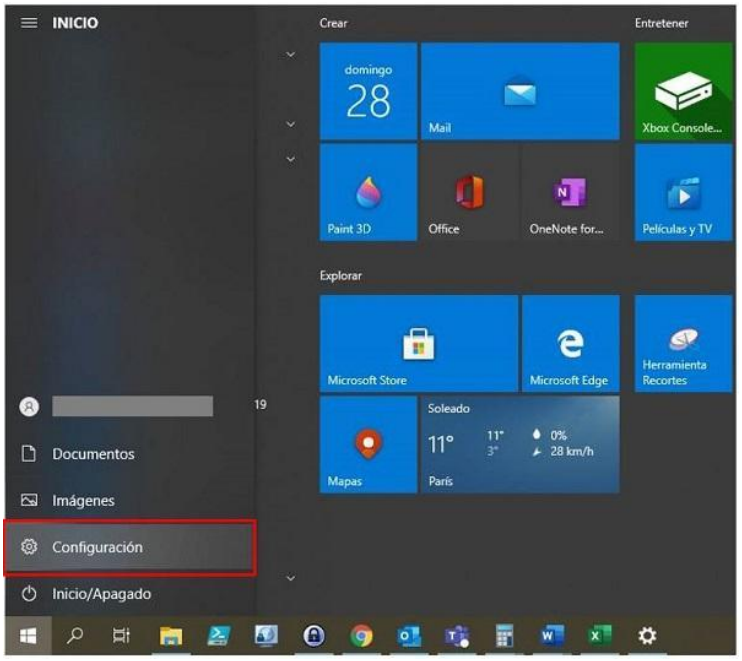
- El nombre de usuario y una contraseña.
- Un indicio de la propia contraseña: puede ser un parte de nuestra
- contraseña o alguna pista que nos ayude a recordarla.

- Respuestas a varias preguntas de seguridad: suelen tratar temas personales, como lugar de nacimiento, nombre de nuestra mascota o aficiones.

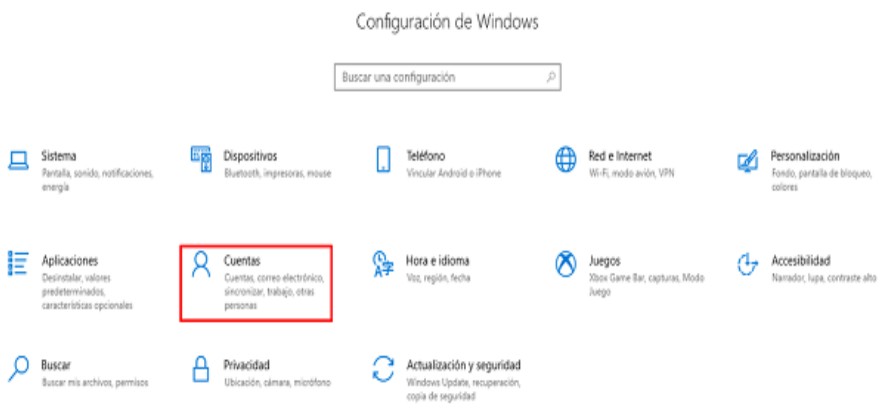
Esta información nos servirá para desbloquear nuestra sesión y recuperar la cuenta en caso de perder u olvidarnos de la contraseña. Cada usuario puede abrir una sesión en Windows, donde utilizar sus herramientas, programas y realizar algunas configuraciones, pero que solo afectan a su sesión (excepto si somos administradores).

Además, podemos configurar las opciones de bloqueo de nuestra sesión:

1. Deberemos hacer clic sobre el icono de **Windows > Configuración.**

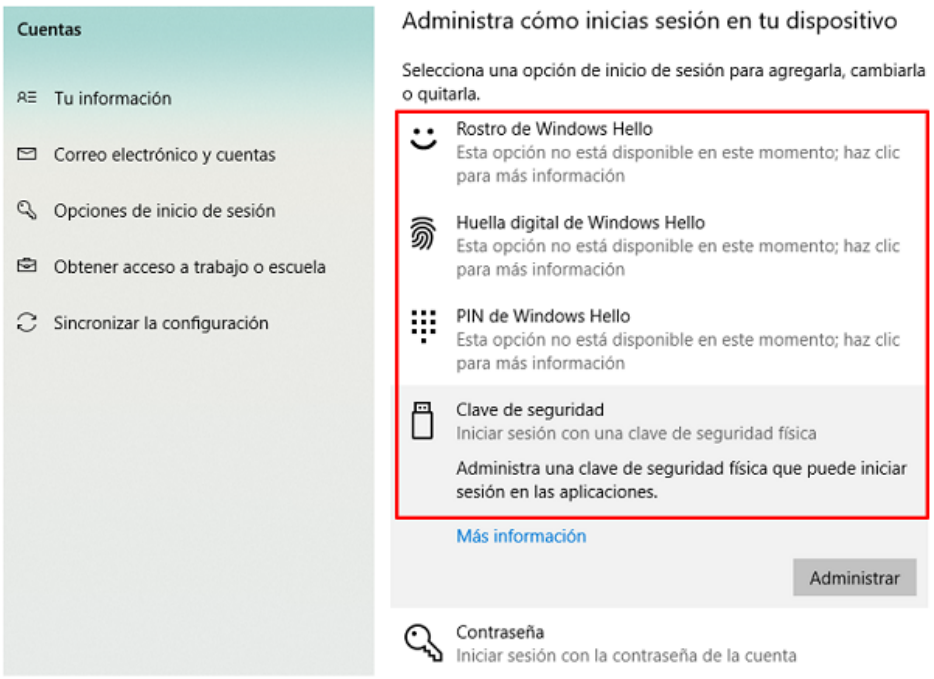


2. Luego, pulsaremos sobre **Cuentas > Opciones de inicio de sesión.**



3. Aquí veremos varias opciones, aunque su disponibilidad dependerá del tipo de ordenador y de si tenemos permisos de administrador:
    - **Rostro de Windows Hello**: podremos utilizar nuestro rostro para bloquear/desbloquear nuestro equipo.
    - **Huella digital de Windows** Hello: en este caso, utilizaremos nuestra huella dactilar.
    - **PIN de Windows Hello**: podremos escoger un código PIN (clave numérica de al menos 4 caracteres), aunque es la opción menos segura.
    - **Clave de seguridad**: se trata de una clave física, que se instala dentro de un dispositivo, como una memoria USB, y que necesitamos conectar al equipo para iniciar sesión.

- **Contraseña**: podremos cambiar la contraseña que creamos junto con la cuenta de usuario, es decir, la que utilizamos para desbloquear el ordenador.



Ordenadores Apple

Los dispositivos con sistema operativo **macOS** (marca Apple) también cuentan con diferentes tipos de cuentas de usuario según los permisos a los que tengan acceso:

- **Administrador**: es una cuenta especial, con permisos para gestionar otras cuentas de usuario, realizar configuraciones del sistema, instalar programas, etc.
- **Estándar**: puede instalar programas y cambiar algunos ajustes del sistema de su cuenta, pero no puede gestionar usuarios.
- **Gestionada con controles parentales**: es una cuenta limitada por el administrador. Este gestiona lo que puede o no puede hacer, como instalar programas, acceder a Internet o a determinadas páginas webs, etc.
- **Solo compartir**: solo puede acceder a los recursos compartidos, como archivos, impresoras, escáneres, etc.
- **Usuario invitado**: solo existe una y sirve para que otros usuarios puedan conectarse a nuestro equipo con permisos muy limitados (no puede instalar programas o cambiar configuraciones). Una vez se cierre la sesión se borrarán todos los archivos generados y datos guardados.

Como forma de proteger el acceso a nuestras cuentas y bloquear nuestros equipos, todas las cuentas utilizan una **contraseña**. En las versiones más modernas de **macOS (Big Sur 11.0)** es posible utilizar otros mecanismos de bloqueo y desbloqueo de nuestra sesión:

- **Touch ID**: Nuestro dispositivo deberá estar dotado de un lector de huella. Esta configuración nos permitirá utilizar nuestra huella dactilar para desbloquear el dispositivo. Para ello:

1. Iremos al menú **Apple > Preferencias del Sistema** y seleccionaremos **'Touch ID'**.
2. Haremos clic en **'Añadir huella'** y, tras introducir nuestra contraseña, seguiremos las instrucciones.

- **Face ID**: del mismo modo, es posible utilizar nuestro rostro para desbloquear nuestros dispositivos. Los pasos serán los mismos, pero seleccionaremos **'Face ID'** en **'Preferencias del Sistema'**.

Finalmente, además de configurar el bloqueo de nuestros dispositivos, hay otra serie de pautas que pueden ayudarnos a mejorar nuestra seguridad:

1. Siempre que dejemos nuestro ordenador o smartphone desatendido, **debemos bloquearlo**.
2. Para añadir una **capa extra de seguridad** podemos utilizar las herramientas por defecto que vienen en todos los sistemas para el cifrado de nuestros dispositivos.
3. Utilicemos contraseñas robustas: entre 8 y 10 caracteres, con mayúsculas y minúsculas, letras y números y caracteres especiales; por ejemplo: *"Micontraseñasegura11"*.
4. **No dejemos nuestro dispositivo sin vigilancia demasiado tiempo cuando haya más personas alrededor,** y tratemos de no usarlo si un desconocido pudiera tener acceso a lo que ocurre en nuestra pantalla (*shoulder surfing*), como cuando vamos en transporte público.

¿Bloqueas todos tus dispositivos cuando terminas de usarlos?