# PLAN DE SEGURIDAD DE UN DISPOSITIVO MÓVIL

Nieves Moreno Aldeguer
@Nieves__moreno

## 1. Justificación

Los dispositivos móviles se han convertido en extensiones de nosotros mismos. Forman parte de nuestro día a día y en ellos almacenamos información valiosa como documentos, vídeos y fotos, y guardamos contraseñas que nos permiten acceder a sitios que contienen información confidencial o personal privada, como cuentas de correo y cuentas bancarias. A pesar de esto, todavía hay muchos dispositivos que no están protegidos adecuadamente y esto puede ser una fuente de problemas de seguridad de los dispositivos móviles.
Es necesario conocer los riesgos y peligros a los que estamos sometidos para poder protegernos lo mejor posible.

## 2. Objetivos del Plan de Seguridad.

**Objetivo general:** Proteger el dispositivo.

**Objetivos específicos:**

1.Proteger los datos.

2. Recuperar datos en caso de pérdida o robo.

3. Localizar el dispositivo en caso de pérdida o robo.

4. Proteger los dispositivos móviles de virus.

## 3. Medidas de control del acceso al dispositivo.

1. Usar un código de desbloqueo.
2. Utilizar Touch ID.
3. Configurar el bloqueo automático después de un tiempo de inactividad.
4. Cambiar la contraseña cada cierto tiempo.

## 4. Medidas de control de los datos compartidos.

1. Desactivar Bluetooth si no lo estamos utilizando.
2. No utilizar redes wifi desconocidas y gratuitas.
3. No compartir ubicación.

4. Desconfíe de archivos adjuntos de correos sospechosos o dsconocidos.

5. No activar enlaces sospechosos que nos lleguen por whatsapp, correo electrónico SMS…

## 5. Medidas de control remoto del dispositivo en caso de robo o pérdida.

1. Control remoto del dispositivo en caso de robo o pérdida.
   En el caso de iOS se utilizará iCloud, que nos permite geolocalizar nuestros dispositivos, bloquearlos en remoto, borrar su contenido o hacer saltar una alarma para encontrarlo en caso de pérdida.

2. Apuntar el IMEI para poder anular el dispositivo (*#06#) y guardarlo en lugar seguro.

## 6. Sobre las actualizaciones del sistema o *apps*.

El malware es una aplicación de software que tiene un objetivo malicioso en el dispositivo móvil donde se instala y se ejecuta sin el consentimiento del usuario. Puede tener objetivos muy variados, siendo los más comunes obtener datos personales y beneficio económico, por ejemplo mediante la suscripción a un servicio SMS premium. Su modo de funcionamiento suele ser automático en modo background y controlado de forma remota desde un servidor, de forma transparente para el usuario.

Para evitar este tipo de programas, sería recomendable tener instalado al menos un antivirus y una herramienta para la detección de malware. Además, sería recomendable seguir las siguientes recomendaciones:

- Instalar aplicaciones sólo de orígenes conocidos.
- Comprobar los permisos antes de instalar/actualizar, especialmente en Android.
- Revisar los comentarios de los usuarios y verificar el desarrollador.

- Instalar aplicaciones que añadan capas de seguridad a los dispositivos móviles, ya sea con métodos de autenticación adicionales más restrictivos, sistemas de copia de seguridad, cifrado de los datos, aplicaciones antivirus y antimalware.
- Actualización automática del sistema operativo y apps favoritas.
- Descargar actualizaciones de lugares seguros.
- Borrar apps que no se utilicen.
- No hacer jailbreak( iPhone) ni rooting (Android)

**6.1. Seguridad física:**

- No perder de vista el dispositivo.

**6.2. Seguridad logística:**

- Evitar instalar aplicaciones cuyos comentarios sean negativos.
- Establecer un código PIN a la SIM distinto al original y guardar en un lugar seguro el código PUK.
- No continuar bulos en aplicaciones de mensajería instantánea reenviándoselo a otros grupos o gente.
- Bloquear el dispositivo mediante contraseña, patrón, huella…
- Instalar alguna app antivirus y herramientas de seguridad.
- Instalar aplicaciones solo de los repositorios oficiales.
- Mantener el sistema operativo actualizado.
- El bloqueo automático debería estar activado.
- Actualizar las aplicaciones a la última versión.
- Realizar copias de seguridad periódicamente.
- No abrir correos electrónicos ni archivos adjuntos de remitentes desconocidos.
- No abrir archivos o enlaces de personas desconocidas enviados por cualquier aplicación de mensajería instantánea.

Precaución a la hora de instalar aplicaciones:

- Evitar instalar aplicaciones de los repositorios no oficiales.
- Evitar instalar aplicaciones con pocas descargas.
- Evitar instalar aplicaciones que solicitan permisos excesivos.
- Evitar instalar aplicaciones cuya valoración por parte de los usuarios sea negativa.

## 7. Copia de seguridad: cómo y cuándo se realizará.

1. Realizar copias de seguridad en iCloud a diario de forma automática.
2. Almacenar información en algunos servicios alojados en la nube: Google Drive, Dropbox, OneDrive…
3. Almacenar copia de seguridad en una memoria externa. Actualizar datos al mes.