

DECÁLOGO DE SEGURIDAD EN DISPOSITIVOS MÓVILES

Posibles riesgos	Medidas a tener en cuenta
Dispositivo sin contraseña/con contraseñas débiles	<ul style="list-style-type: none">- Tener un PIN no predecible- Activar el código de desbloqueo (número, huella dactilar...) robusto- Bloqueo automático tras un breve tiempo sin usar el dispositivo- Cambiar las contraseñas periódicamente- No recordarlas en el navegador
Wifis públicas/abiertas	<ul style="list-style-type: none">- No activar la conexión automática a wifis públicas/abiertas- No conectarse a redes abiertas en lugares públicos- Borrar los datos cuando se salga de la wifis pública- Eliminar el historial periódicamente- Si se conecta: no utilizar usuario/contraseña, ni datos sensibles
Transmitir información personal a desconocidos	<ul style="list-style-type: none">- No dar o mostrar información de nuestra vida privada (gustos, domicilio, vacaciones...)- Tener consentimiento de las demás personas que salen en la foto
Geolocalización	<ul style="list-style-type: none">- Sólo activar cuando sea necesario
Malware/virus	<ul style="list-style-type: none">- Mantener actualizado el sistema operativo y las apps- Tener instalado un antivirus en el dispositivo- Usar software especializado (como Conan Mobile)- No abrir mensajes o enlaces de desconocidos

Apps fraudulentas	<ul style="list-style-type: none">- Descargar sólo de repositorios oficiales- Observar su procedencia, si tiene muchas descargas, su valoración...- Revisar los permisos necesarios (¿son de verdad necesarios?)- Usar software especializado (como Conan Mobile)
Información errónea o falsa	<ul style="list-style-type: none">- Comprobar el dominio de la web- Fijarse en el candado que aparece en la barra de navegación- Sospechar de “errores” en la página (nombres casi parecidos...)- Comprobar el certificado de seguridad- No creer en los “chollos” que se ofrecen
Pérdida de información	<ul style="list-style-type: none">- Hacer una copia de seguridad periódicamente
Información sensible en el dispositivo	<ul style="list-style-type: none">- Tener cifrado el dispositivo y la memoria extraíble para que los daos no puedan ser accesibles por terceros
Pérdida o robo	<ul style="list-style-type: none">- Instalar una app de rastreo, bloqueo y borrado remoto del dispositivo

