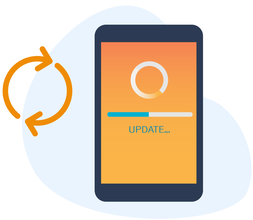
# Seguridad en el móvil corporativo

Gran parte de las medidas de seguridad necesarias para el buen funcionamiento de los móviles corporativos de un organismo se deben implantar desde la propia organización, pero existen acciones o buenas prácticas que deben ser realizadas por los propios usuarios.




**1. Actualiza siempre tanto el sistema operativo como las aplicaciones**: las actualizaciones incluyen importantes parches de seguridad que subsanan vulnerabilidades descubiertas.

**2. Configura el desbloqueo por huella dactilar**. Es un método de acceso cómodo y difícil de replicar. El reconocimiento facial también es una buena opción.

**3. Controla los permisos de las aplicaciones**. Las apps solicitan acceder a ciertos datos del terminal como ubicación, cámara, micrófono, contactos o mensajes de texto, pero eres tú quien tiene la última palabra.

**4. Aprende a distinguir publicidad y notificaciones**. Es importante recibir notificaciones relevantes (por ejemplo, correo o mensajería corporativa), pero recibir un número inusual de notificaciones (publicidad o noticias) indica que no hemos gestionado correctamente los permisos o que tenemos aplicaciones con un comportamiento anómalo. Si fuera el caso, revisa las aplicaciones instaladas y los permisos de cada una, además de las webs a las cuales has permitido mostrar

**5. No utilices VPN diferentes de la corporativa**. Las VPN hacen que tus comunicaciones lleguen a los servidores de una organización, donde se procesan y protegen antes de continuar su camino hacia Internet. Las VPN gratuitas, probablemente, lo hagan a cambio de utilizar tus datos.


**6. Almacenamiento de datos corporativos en el móvil**. Aunque los móviles tienen cada vez más funcionalidades, tanto por seguridad como usabilidad, no son la herramienta idónea para procesar ni almacenar documentos o información corporativa. En caso de descargarla en un móvil corporativo, es recomendable eliminarla tras su consulta. Igualmente, recordamos que no es conveniente tratar datos corporativos en dispositivos personales.

**7. Si le sucede algo a tu dispositivo, repórtalo**. Si sospechas que el móvil puede estar infectado, si lo pierdes, o si le sucede algo a la tarjeta SIM, repórtalo al Servicio correspondiente en tu organismo para que puedan tomar las medidas oportunas.

Con estas recomendaciones, protegerás la información de tu móvil corporativo y tus datos personales.

GENERALITAT VALENCIANA
Conselleria d'Hisenda, Economia i Administració Pública

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

csirtcv.gva.es
concienciat.gva.es