

Seguretat en el mòbil corporatiu

Gran part de les mesures de seguretat necessàries per al bon funcionament dels mòbils corporatius d'un organisme s'implanten des de la mateixa organització, però hi ha accions o bones pràctiques que han de ser realitzades pels usuaris.



1. Actualitza sempre tant el sistema operatiu com les aplicacions: les actualitzacions inclouen importants pegats de seguretat que esmenen vulnerabilitats descobertes.



2. Configura el desbloqueig per empremta dactilar. És un mètode d'accés còmode i difícil de replicar. El reconeixement facial també és una bona opció.

3. Controla els permisos de les aplicacions.

Les app sol·liciten accés a algunes dades del terminal com ara ubicació, càmera, micròfon, contactes o missatges de text, però eres tu qui té l'última paraula.

4. Aprén a distingir publicitat i notificacions.

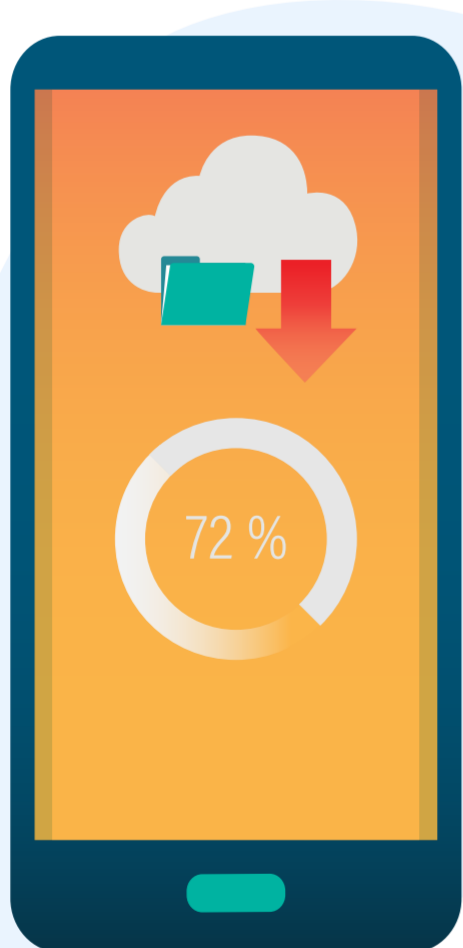
És important rebre notificacions rellevants (per exemple, correu o missatgeria corporativa), però rebre un nombre inusual de notificacions (publicitat o notícies) indica que no hem gestionat correctament els permisos o que tenim aplicacions amb un comportament anòmal. Si fora el cas, revisa les aplicacions instal·lades i els permisos de cadascuna, a més de les webs a les quals has permès mostrar notificacions en el navegador.



5. No utilitzes VPN diferents de la corporativa.

Usar una VPN fa que totes les teues comunicacions arriben als servidors d'una empresa o organització, on es processen i protegeixen abans de continuar el seu camí cap a internet. Les VPN gratuïtes, probablement ho fan a canvi d'usar les teues dades.

6. Emmagatzematge de dades corporatives en el mòbil. Encara que els mòbils tenen cada vegada més funcionalitats, tant per seguretat com usabilitat, no són la ferramenta idònia per a processar ni emmagatzemar documents o informació corporativa. En cas de descarregar-la en un mòbil corporatiu, és recomanable eliminar-la després de la seua consulta. Igualment, recordem que no és convenient tractar dades corporatives en dispositius personals.



7. Si li passa alguna cosa al teu dispositiu, informa. Si sospites que el mòbil pot estar infectat, si el perds, o si li passa alguna cosa a la targeta SIM, informa'n al Servei corresponent del teu organisme perquè puguen prendre les mesures oportunes.



Amb estes recomanacions, protegiràs la informació del teu mòbil corporatiu i les teues dades personals.