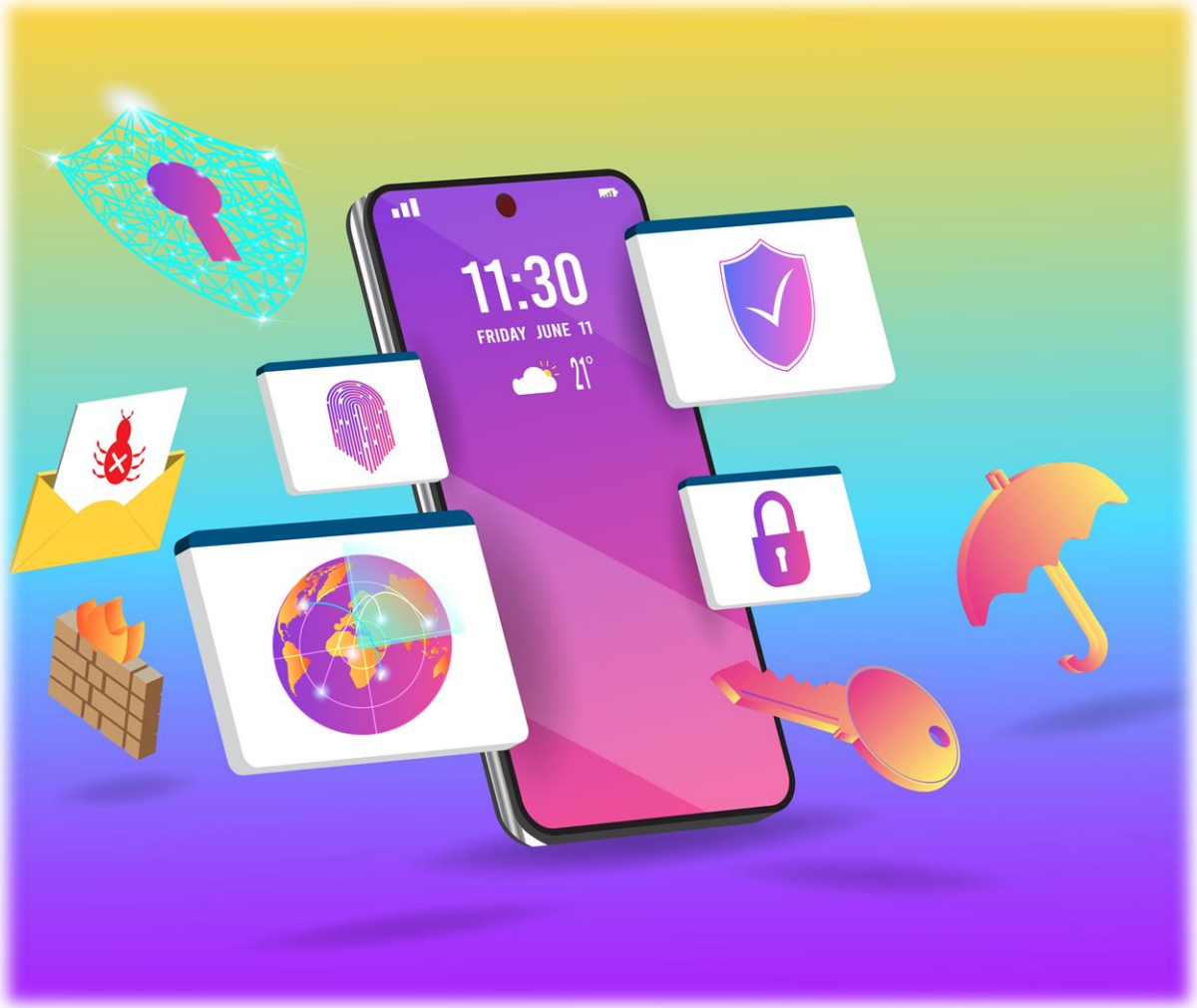
Govern d'Andorra

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

Ús de dispositius mòbils

Conscienciació en ciberseguretat

Maig de 2022



ÍNDEX

Comporta riscos l'ús de dispositius mòbils?

L'ús de dispositius mòbils ha crescut considerablement degut a la millora dels serveis de telecomunicacions, així com les capacitats tècniques dels mateixos dispositius. Aquesta evolució ha suposat un potenciador del seu ús en l'àmbit laboral, permetent-nos acomplir pràcticament qualsevol tasca en situacions de mobilitat de manera senzilla i còmoda.

Però no tot són avantatges pel que fa a l'ús dels dispositius mòbils tant en el món personal com professional. De fet, l'exposició a algunes amenaces és major a causa de les seves característiques i modalitat d'ús.

En el context professional, l'ús de dispositius corporatius o inclús personals (si es permet), pot comportar situacions de risc com les següents:

- Coexistència d'aplicacions d'ús personal (potencialment insegures) i corporatives.
- Segregació deficient entre dades personals i corporatives.
- Alternança en la connexió a xarxes corporatives i xarxes externes (potencialment insegures).
- Accés a recursos corporatius des de dispositius amb una configuració insegura.

Comporta riscos l'ús de dispositius mòbils?

Pèrdua, robatori o destrucció de dispositius

L'evolució dels dispositius mòbils els fa cada vegada més petits, lleugers i manejables, característiques d'ús que els fan més útils i còmodes però, a la vegada més fràgils.

La pèrdua, robatori o trencament d'un dispositiu mòbil no sols implica la pèrdua econòmica que costi la seva reposició o reparació, sinó que també posa en risc la seguretat de la informació confidencial de l'empresa o personal (segons el dispositiu i ús que li donem).

En cas de pèrdua o robatori, podria donar-se un accés no autoritzat a la informació emmagatzemada, així com a altres recursos, considerant que podríem trobar-nos amb debilitats en el control d'autenticació (no requerint sempre una autenticació forta de l'usuari).

Robatori de credencials

Els dispositius mòbils i les aplicacions instal·lades en aquests, tenen implementats en moltes ocasions controls d'autenticació que emmagatzemen o possibiliten l'emmagatzematge de les credencials utilitzades pels usuaris.

Encara que aquestes credencials es registren normalment de manera intel·ligible (aplicant algoritmes de "hasheo"), un atacant avançat podria arribar a aconseguir les credencials en clar fent ús d'eines i tècniques avançades.

El robatori de credencials és un risc crític perquè els atacants no sols podran realitzar accions il·lícites, sinó que podria dificultar-se la seva detecció si les desenvolupen de forma prèviament estudiada.

1. Comporta riscos l'ús de dispositius mòbils?

Comporta riscos l'ús de dispositius mòbils?

Mal ús del dispositiu

L'usuari és, a parts iguals, el risc més gran i la millor eina pel que fa a la seguretat, ja que és qui finalment gestiona, modifica i utilitza la informació corporativa.
Un usuari que utilitzi el dispositiu mòbil en l'àmbit laboral ha d'estar conscienciat i format en els riscos que deriven del seu ús i obrar conforme a les polítiques de seguretat establides per l'empresa per no caure en accions que poden afectar a la informació com: Instal·lació d'aplicacions insegures provinents de fonts o "Markets" no oficials i puguin contenir programari maliciós o "Malware".
Canvis en la configuració que atorguen majors permisos d'accessos a la informació a aplicacions no corporatives o no protegides.
Manipulació dels dispositius per eliminar la configuració i limitacions de fàbrica.

Connexió a xarxes insegures

Per les seves característiques de mobilitat, serà més probable que els dispositius mòbils puguin connectar-se a xarxes públiques, alienes a l'organització o al nostre context habitual. Aquestes xarxes alienes comporten una exposició a diversos ciberatacs per suplantació de la xarxa, de dispositius, dels llocs web, afecció de serveis de resolució de direccions, o per intercepció de las comunicacions.

Com més ampli sigui el públic al qual està dirigit l'ús de la xarxa i menor sigui el nivell de seguretat aplicat (ús de protocols segurs, restricció d'accés a dispositius preautoritzats, control de sessions vàlides, etc.) més probabilitats hi haurà que la xarxa sigui compromesa o estigui exposada a riscos.

ÍNDEX

2. Mesures de protecció

Generals per l'usuari

Codi d'accés i bloqueig del dispositiu

Donat que l'ús dels dispositius mòbils es dona en gran part fora de les instal·lacions, és necessari aplicar mesures de seguretat relatives al bloqueig i accés del terminal. S'han d'aplicar les mesures establertes en la política de contrasenyes i accés de l'empresa, configurant un bloqueig del dispositiu per inactivitat, varis nivells d'autenticació i bloqueig del dispositiu en cas d'introducció de credencials invàlides de forma reiterativa.

Aplicacions instal·lades

Els dispositius mòbils tindran accés a informació i serveis corporatius a través d'aplicacions instal·lades en aquests. És important instal·lar únicament aplicacions confiables i controlar l'accés de totes elles tant a nivell de recursos del dispositiu (agenda, emmagatzematge, etc.) com a nivell dels serveis públics amb els quals es connecten. D'aquesta manera mitigarem incidents derivats d'accessos no autoritzats.

Emmagatzematg e al núvol

L'emmagatzematge en el núvol és una solució molt útil per a garantir la seguretat de les dades corporatives. En aquest context passa a ser especialment important la utilització de serveis que ofereixin garanties, i una configuració adequada de la connexió o aplicació client (instal·lada en el mòbil) perquè totes les comunicacions es realitzin de manera segura.

Generals per l'usuari

Còpies de seguretat

És cert que la informació tractada pels mòbils sol quedar emmagatzemada en les aplicacions-serveis al núvol, no sempre és així. Inclús les mateixes configuracions podrien ser importants si esperem recuperar el dispositiu ràpidament davant una pèrdua. En aquestes situacions és crucial aplicar una política de còpies de seguretat als dispositius mòbils.

Xifratge de dispositius

Els avantatges de mobilitat que ofereixen aquest tipus de dispositius tenen com contrapartida un major risc d'accessos no autoritzats per pèrdues o robatoris. De la mateixa manera que ho fem amb equips portàtils o discs durs extraïbles, el xifratge de la unitat de l'emmagatzematge és possible i molt recomanable per mitigar aquest risc.

Actualització de dispositius

Els dispositius mòbils estan en constant canvi, el seu creixement en l'àmbit tecnològic i operacional és exponencial i cada vegada compta amb més eines, el que comporta de manera directa majors riscos. És necessari mantenir actualitzat el dispositiu en la seva última versió del sistema operatiu, així com les actualitzacions de seguretat que els desenvolupadors d'aplicacions llencen periòdicament.

Generals per l'usuari

Configuració mínima de seguretat

Tant l'empresa com l'usuari han de prendre mesures quant a la configuració d'un dispositiu mòbil quan aquest tingui accés a la informació sensible corporativa, limitant accessos segons els privilegis, deshabilitant permisos de les aplicacions, limitant les connexions a xarxes insegures i instal·lació automàtica, bloquejant la sincronització amb el núvol si no estem connectats a xarxes corporatives...

Connexions a xarxes segures

L'ús del dispositiu mòbil fora de l'entorn de l'empresa és cada dia més habitual. Això pot provocar que ens connectem a xarxes públiques o insegures en situacions en les quals no tinguem elecció. És molt important l'ús de les xarxes segures VPN corporatives i, en cas de no disposar d'elles, xarxes mòbils 3G, 4G o 5G. Quan hàgim d'accedir a una xarxa pública insegura ho farem conforme a la política de seguretat corporativa.

ÍNDEX

2. Mesures de protecció

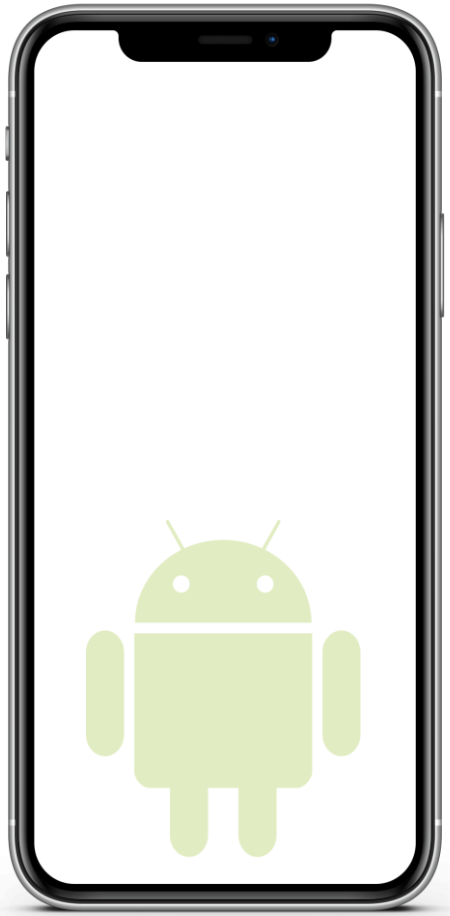
Actualitza el software
Mantingues el teu dispositiu actualitzat!
Ajustaments > Sobre el telèfon > Actualització de software > Descarregar actualització

Estableix contrasenyes segures, desbloqueig biomètric i doble factor d'autenticació
Disposa de diferents mesures de seguretat per evitar l'uso de tercers
Ajustaments > Seguretat i Ubicació > Bloqueig de pantalla/Contrasenya/Patró/Empremta digital/Reconeixement facial
Ajustaments > Google > Gestionar el teu compte de Google > Seguretat > Doble factor d'autenticació

Xifrat
Xifra la informació emmagatzemada en el teu dispositiu
Ajustaments > Seguretat i Ubicació > Xifrar emmagatzematge de targeta SD

Copies de seguretat
Configura les copies de seguretat automàtiques
Ajustaments > Google > Fer copia de seguretat

Android



Permisos d'apps
Gestiona els permisos d'accés a informació de les aplicacions
Ajustaments > Aplicacions > Permisos

Ubicació
Desactiva la ubicació per evitar el seguiment de la teva informació
Ajustaments > Ubicació > Utilitzar Ubicació

Localitzar el meu dispositiu
Habilita l'opció de localització del dispositiu de forma remota en cas de pèrdua
Des del teu compte Google: Localitza el meu dispositiu

Esborrat segur
Sigui de memòria, comptes o restabliment del dispositiu
Ajustaments > Emmagatzematge > Targeta SD > Formatar
Ajustaments > Comptes > Selecciona el teu compte > Eliminar
Ajustaments > General > Restablir dades de fàbrica

ÍNDEX

Configurar sistema de desbloqueig de dispositiu per biometria o una contrasenya segura

Codi PIN: *Configuració > Touch ID / Face ID i codi > Activar codi.*

Empremta dactilar: *Configuració > Touch ID i codi > Afegir una empremta*

Reconeixement facial: *Configuració > Face ID i codi > Configuració Face ID*

Activar doble factor d'autenticació

iOS 10.3 o superior: *Configuració > [nom] > Contrasenya i seguretat > Activar autenticació de doble factor > Continuar*

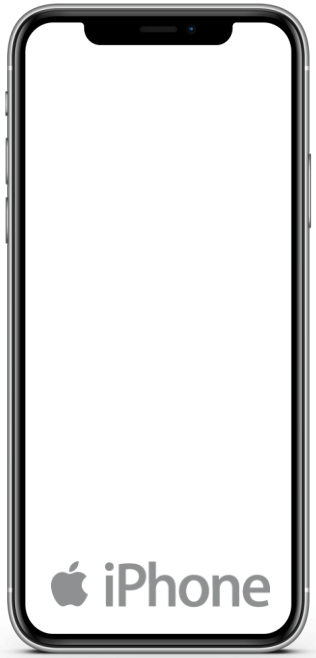
iOS 10.3 o superior: *Configuració > iCloud > [Apple ID] > Contrasenya i Seguretat > Activar autenticació de doble factor i seguir passos indicats*

Configurar còpies de seguretat

Recolza la informació emmagatzemada en el dispositiu al iCloud.

Configuració > [nom] > [seleccionar el dispositiu] (en cas de tenir varis dispositius associats al compte) > Copia en iCloud > Habilita l'opció de Còpia en iCLoud

iPhone



Desactivar connexions sense fils

No mantinguis les connexions sense fils del dispositiu activades si no estan en ús.

Configuració > Wifi / Punt d'accés personal / Bluetooth

La tecnologia NFC no pot ser desactivada, important tancar l'aplicació Apple Pay quan deixa de ser utilitzada.

Assegura't que el dispositiu està actualitzat

Executa les actualitzacions rebudes via notificació i revisa si hi ha actualitzacions pendents en: *Configuració > General > Actualització de software > Descarregar i instal·lar*

Instal·lació i gestió d'aplicacions

A l'instal·lar aplicacions utilitza la botiga oficial d'App Store i revisa les opinions i valoracions sobre el desenvolupador, i elimina les aplicacions que ja no utilitzis.

Revisar els permisos assignats a les apps

Accedeix a Configuració, al final de la pantalla es mostra el llista de apps instal·lades amb els seus permisos assignats.

Esborrat segur

Si deixes d'utilitzar el dispositiu de forma permanent has d'executar una eliminació segura del seu contingut.

Configuració > General > Restablir i polsar sobre Esborrar continguts i Configuracions

Govern d'Andorra

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

ANDORRA
DIGITAL

Entitats col·laboradores

andorra
telecom

DAND
DIGITALAND by Ibermática | TIN