CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

BONES PRÀCTIQUES EN DISPOSITIUS MÒBILS

Document Públic

setembre de 2020

GENERALITAT VALENCIANA
Conselleria d'Hisenda i Model Econòmic

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

UNIÓ EUROPEA
Fons Europeu de Desenvolupament Regional
Una manera de fer Europa

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

CSIRT-CV és el Centre de Seguretat TIC de la Comunitat Valenciana. Naix el juny de l'any 2007 com una aposta de la Generalitat Valenciana per la seguretat en la xarxa. Va ser una iniciativa pionera en ser el primer centre d'aquestes característiques que es va crear a Espanya per a un àmbit autonòmic.

Índex de continguts

1. Introducció i objectius

Les noves tecnologies, en la seua constant evolució, han permés que es desenvolupen noves eines per a realitzar labors professionals de manera més eficaç. S'ha evolucionat de l'ordinador com a principal eina de treball a utilitzar dispositius mòbils, com telèfons intel·ligents o tauletes tàctils, en entorns de treball en què la mobilitat és fonamental.

No obstant això, aquesta **mobilitat comporta riscos** associats a la possibilitat de pèrdua o robatori del dispositiu, en què es produeix una pèrdua de confidencialitat de la informació que conté.

Aquest document pretén recopilar una sèrie de recomanacions bàsiques o **bones pràctiques d'ús de telèfons intel·ligents i tauletes tàctils** amb la finalitat d'aportar mesures de seguretat adequades perquè la informació emmagatzemada en els dispositius estiga segura. Aquestes recomanacions seran personalitzades per als sistemes operatius més estesos en aquest tipus de dispositius: **Android**[1] i **iOS**[2].

1 *https://www.android.com/*
2 *https://www.apple.com/es/ios/*

2. Bones pràctiques

A continuació, s'enumeraran les mesures disponibles que es poden dur a terme per a incrementar la seguretat en els dispositius mòbils per a cada un dels sistemes operatius d'ús més freqüent.

2.1. Seguretat lògica

2.1.1. Bloqueig per contrasenya

La major part de dispositius disposa de mesures de bloqueig quan entren en mode d'espera. Aquest recurs garanteix que l'accés a l'ús del terminal només el pot efectuar la persona autoritzada que coneix la clau. En cas de pèrdua o robatori, l'única manera de poder utilitzar el dispositiu és restaurant els valors de fàbrica, per la qual cosa tota la configuració i les dades emmagatzemades es perdrien.

Hi ha diversos mètodes per a restringir l'ús del dispositiu. Aquests varien segons el fabricant. Els més utilitzats **són la contrasenya amb PIN de 4 dígits, contrasenya alfanumèrica o patró de desbloqueig**.

És important, igualment, configurar el terminal perquè passat **un cert temps d'inactivitat passe automàticament a mode d'espera i s'active el bloqueig de la pantalla**. Si no s'usa aquesta mesura, la tècnica de bloqueig perd pràcticament tota l'efectivitat.

2.1.1.1. Bloqueig per contrasenya en Android

En terminals amb Android, per a afegir una contrasenya o patró de desbloqueig, s'han de seguir els passos següents:

Dins del menú principal cal seleccionar **Configuració**, buscar l'apartat de **Pantalla bloqueig** i després accedir a **Tipus de bloqueig de pantalla.**

En aquest apartat es pot activar aquesta protecció de pantalla, que pot ser, per mitjà d'un patró de moviment, que s'ha de fer amb el dit en la pantalla, un PIN numèric de 4 xifres, una contrasenya de 4 caràcters i, en alguns models de dispositius, es pot fer ús de l'empremta digital.

En aquest mateix apartat també es pot configurar quan es vulga bloquejar el dispositiu, si de manera immediata o al cap d'uns pocs minuts després d'un període d'inactivitat.

Es recomana no mostrar visiblement en la nostra pantalla el nostre PIN, contrasenya o patró de desbloqueig mentre desbloquegem el nostre terminal per a evitar que un tercer puga veure'ns mentre ho fem, per a això en aquest apartat de Seguretat es pot

desactivar aquesta opció.

En algunes tauletes tàctils per a configurar una pantalla de bloqueig es pot fer en **Configuració/Ubicació i Seguretat/Configura pantalla de bloqueig.** En fer clic s'obtindran les opcions de posar un patró de moviment, un PIN o una contrasenya.

2.1.1.2. Bloqueig per contrasenya en iOS

En iPhones o iPads es pot afegir una contrasenya d'accés al dispositiu de la manera següent:

Dins del menú principal navegue fins a Configuració i, una vegada dins, cal seleccionar l'apartat **General**, allí seleccionar **Bloqueig amb codi** o **Touch Id i codi depenent del model** en què es pot afegir un PIN de 4 xifres de manera que cada vegada que s'accedisca al nostre dispositiu s'haurà de marcar aquest codi.

Es pot també activar un camp (**Esborrar dades**) en què després de marcar erròniament determinades vegades un codi, el contingut del dispositiu s'esborrarà de manera immediata, però és una acció que no es recomana. És important, a més, evitar que en teclejar el PIN per a accedir al dispositiu aquest siga vist per un tercer.

En **Configuració/General** es pot activar bloqueig automàtic i triar el temps (es recomana 5 minuts) després del qual si el dispositiu ha estat inactiu es bloqueja de manera automàtica. El dispositiu no ha de tindre període de gràcia per a accedir-hi sense clau. Així que en **Configuració/General** en **Bloqueig amb codi** s'ha de tindre en l'opció **Sol·licitar** el valor IMMEDIATAMENT.

2.1.2. Encriptació de la memòria

Aquesta pràctica se sol complementar amb la tècnica anterior. Consisteix a encriptar la memòria d'emmagatzematge, i així impossibilitar la còpia o extracció de dades si no es coneix la contrasenya de desbloqueig.

Segons el model, es permet encriptar **tant la memòria interna** com **la memòria d'emmagatzematge extern**, com són les targetes de memòria flaix. Una vegada encriptat, només es podrà accedir a les dades emmagatzemades en encendre el dispositiu amb la contrasenya de bloqueig de pantalla.

Si no es coneix la clau, serà molt difícil recuperar la informació, encara que s'utilitzen tècniques forenses d'extracció i còpia de dades. L'única manera possible seria amb tècniques de força bruta, que consisteixen a provar automàticament totes les combinacions possibles de contrasenya, fins a trobar la que permet accedir-hi.

Per tant, és important que, per tal que aquest atac no puga dur-se a terme, s'utilitze una contrasenya complexa, que combine lletres amb dígits, majúscules i caràcters especials.

2.1.2.1 Encriptació de la memòria en Android

Android disposa d'un sistema d'encriptació del sistema d'arxius del dispositiu a partir de la versió Android 3.0 Honeycomb.

Requereix que l'usuari introduïsca una contrasenya o PIN (en aquest cas, no podrem posar com a bloqueig per pantalla un patró de moviment, ja que no està permés que s'use per a encriptar la memòria) com a bloqueig de pantalla, que s'utilitzarà per a generar una clau que s'usa per a encriptar el sistema d'arxius.

És important triar una contrasenya robusta que incloga lletres i xifres perquè la clau d'encriptació que es genere siga igualment robusta. Per a activar l'encriptació del dispositiu se seguiran els passos següents:

En **Configuració**, es navegarà fins a **Seguretat** i s'ha d'activar l'opció **Encripta el dispositiu**. Es podrà encriptar comptes, configuració, aplicacions descarregades i les seues dades, multimèdia i altres arxius. Una vegada encriptat el dispositiu, es necessitarà un PIN o contrasenya per a desencriptar-lo cada vegada que s'encenga.

És important assenyalar que una vegada encriptat el dispositiu el rendiment del dispositiu es pot veure reduït i no és possible tornar a deixar-lo com estava, llevat que es restaure de fàbrica.

2.1.2.2 Encriptació de la memòria en iOS

En iOS, en fixar un codi d'accés, el dispositiu protegeix per defecte la informació de les aplicacions mitjançant una clau d'encriptació derivada d'aquest codi. Si tenim activat el codi de bloqueig, Apple l'utilitza juntament amb una clau de 256 bits única emmagatzemada en el maquinari del dispositiu per a encriptar les nostres dades, com el correu electrònic.

Cap persona sense autorització podrà, per tant, extraure informació personal del dispositiu. Per a assegurar-nos que això no ocorre, s'ha de fer el següent: En Configuració/General/Bloqueig amb codi ha de mostrar-se el missatge "La protecció de dades està activada" a la part inferior de la finestra.

2.1.3 Esborrament remot

Amb aquesta pràctica es podran esborrar les dades del dispositiu i restaurar-les als valors de fàbrica, tot això de manera remota. Pot ser molt important tindre a mà aquest recurs en cas de pèrdua o robatori del dispositiu, sobretot si la informació emmagatzemada és sensible. Aquesta funció depén del tipus de dispositiu, del fabricant o de l'operadora, i és possible que el servei siga de pagament.

2.1.3.1 Esborrament remot en Android

Google ofereix un servei d'eliminació remota de dades d'un dispositiu mòbil per a Google Apps for Business, Google Apps for Education i Google Apps for Government;

si el seu usuari ha configurat Google Sync en un dispositiu mòbil compatible o en un dispositiu Android que tinga instal·lada l'aplicació Política de dispositius de Google Apps, es pot usar el quadre de comandament de Google Apps per a eliminar les dades del dispositiu de manera remota.

L'esborrament suprimeix totes les dades emmagatzemades en el dispositiu (correu, calendari, contactes, etc.) però no elimina les emmagatzemades en la targeta SD del dispositiu. Per a poder esborrar un dispositiu de manera remota, primer hem de localitzar el dispositiu, per a això han de complir-se una sèrie de condicions:

- Haver afegit un **compte de Google** en el dispositiu, amb la qual cosa, ja tindrem activat per defecte "Troba el meu dispositiu". A més, ha de tindre la **sessió iniciada**.
- Ha d'**estar encés**.
- **Connectat a una xarxa de dades** mòbils o WI-FI.
- Ha de tindre **activada la ubicació**.

Si disposem d'un altre dispositiu Android, podem instal·lar-hi l'aplicació "Troba el meu dispositiu", disponible en la botiga **Play Store**.

Una altra opció és accedir a aquesta web[3] des d'un altre dispositiu o des d'un ordinador i seguir aquests passos:

1. Ací hem d'**iniciar sessió en el compte de Google** que sabem que està activa en el dispositiu perdut/robat. Si tenim diversos dispositius configurats amb aquest compte de Google, hem de triar el dispositiu que volem localitzar, a la part superior de la pantalla.

2. El **telèfon perdut rebrà una notificació**.

3. En el **mapa podrem veure la ubicació aproximada** d'on es troba el dispositiu en aquest moment o de la seua última ubicació coneguda.

4. Ara hem de fer **clic en "Habilita bloqueig i esborrament"**, per a decidir què volem que succeïsca:

   * **Reprodueix un so**, amb això fem que el telèfon sone a volum màxim durant 5 minuts, encara que estiga en silenci o vibració.

   * **Bloqueja el dispositiu**, amb això fem que es bloquege amb el PIN, patró o contrasenya que tinguem establit, i en cas que no n'hàgem configurat cap, podem fer-ho en aquest moment.

   * **Esborra el contingut del dispositiu**, perquè elimine definitivament totes les dades del telèfon, encara que pot ser que no elimine les dades

3 https://www.google.com/android/find

de la targeta SD. Però si usem aquesta opció, després ja no podrem utilitzar Troba el meu dispositiu. A més, si trobem el dispositiu després d'haver esborrat les dades, és possible que necessitem la contrasenya del compte de Google per a poder tornar a usar-lo.

2.1.3.2 Esborrament remot en iOS

Apple ofereix la funció "**Buscar el meu iPhone**",[4] aplicació gratuïta que permet des d'un altre iPhone, iPad o iPod Couch, o utilitzant un navegador web per a Mac o PC amb una sessió iniciada en www.icloud.com15 diverses opcions, entre les quals hi ha l'esborrament de tot el contingut i les dades del dispositiu restaurant la configuració de fàbrica.

Per a poder usar les seues característiques, la funció "Buscar el meu iPhone" ha d'estar activada en la configuració d'iCloud en el dispositiu.

Aquesta funció només pot estar activada en un compte. Per a activar aquesta funció s'ha d'accedir a **Configuració/iCloud i activar "Buscar el meu iPhone"**.

2.1.4 Còpies de seguretat

Si la informació utilitzada en el dispositiu és important, i la seua pèrdua ocasiona problemes greus, aleshores és convenient utilitzar alguna solució de còpies de seguretat.

Hi ha programes que sincronitzen les dades emmagatzemades amb l'ordinador d'escriptori, o en alguna aplicació en línia que ofereix el fabricant, de manera que les dades estan sempre disponibles i actualitzades. En aquesta pàgina[5] es poden trobar eines per a fer còpies de seguretat.

En cas de pèrdua del terminal, la informació continuaria estant disponible i fora de perill. Es recomana que si s'utilitzen aquest tipus d'opcions, de sincronitzar les nostres dades amb alguna aplicació en línia externa a la nostra organització, no se sincronitze la informació confidencial, si n'hi ha, ja que deixaria d'^estar a les nostres mans'. El més recomanable és trobar solucions de còpies de seguretat controlades per l'organització perquè la informació no viatge fora d'aquesta.

2.1.4.1 Còpies de seguretat en Android

Google no disposa d'un servei de còpies de seguretat dels arxius de dades o multimèdia del dispositiu, per a això caldria usar aplicacions de tercers. Però sí que permet copiar la configuració del dispositiu (contrasenyes de les xarxes Wi-Fi, favorits, dades d'aplicacions, opcions de configuració) en els servidors de Google. Els passos que cal seguir són els següents:

- En **Configuració/Privadesa** marcar l'opció de **Copia la meua configuració**. En algunes tauletes tàctils haurem d'anar a **Configuració/Privadesa** i marcar l'opció de **Fes còpia de seguretat del compte**.

4 https://apps.apple.com/es/app/buscar-mi-iphone/id376101648
5 https://www.osi.es/es/herramientas-gratuitas?combine=&herramienta_selec%5B%5D=124

2.1.4.2 Còpies de seguretat en iOS

A través d'iCloud i iTunes es poden fer còpies de seguretat de la major part de les dades de l'iPhone o iPad (fotos, configuració del dispositiu, com ara comptes de correu o contactes, missatges, etc.).

Els passos que cal seguir perquè iCloud realitze de manera automàtica una còpia de seguretat de les dades més importants del dispositiu són els següents:

- Anar a **Configuració/iCloud/Emmagatzematge i còpies**

La còpia de seguretat s'executarà diàriament sempre que el dispositiu:

- Estiga connectat a Internet via Wi-Fi.
- Estiga connectat a una font d'alimentació.
- Tinga la pantalla bloquejada.

És possible fer una còpia de seguretat de manera manual sempre que el dispositiu estiga connectat a Internet via Wi-Fi seleccionant "Realitzar còpia de seguretat ara" en **Configuració/iCloud/Emmagatzematge i còpies**.

2.2. Els perills del *malware* (programari maliciós)

L'ús cada dia més freqüent de telèfons intel·ligents i tauletes tàctils ha derivat en què la creació de *malware* apunte cap a aquestes plataformes. Hui dia el risc que un telèfon intel·ligent puga ser infectat per un virus és una realitat.

Aquests es basen principalment en el robatori de documents, contrasenyes, dades bancàries i informació personal. Per això és convenient adoptar unes mesures de seguretat per a evitar en la mesura que siga possible infeccions de *malware* que faça perillar la confidencialitat, integritat i disponibilitat de la informació.

Es recomanen les lectures de les nostres campanyes de conscienciació "Seguretat en Aplicacions mòbils"[6] i "Seguretat en dispositius mòbils"[7].
A continuació, alguns consells importants sobre això.

2.2.1 Fonts de confiança

El principal problema d'infeccions en dispositius mòbils té l'origen en la instal·lació de programes des de fonts desconegudes.

És molt important instal·lar aplicacions únicament des dels repositoris oficials del dispositiu, com App Store i Google Play, per a iPhone/iPad i Android, respectivament.

6 https://concienciat.gva.es/va/tips_de_seguretat/seguretat-en-aplicacions-mobils/
7 https://concienciat.gva.es/va/tips_de_seguretat/seguretat-en-dispositius-mobils/

S'ha d'evitar sempre instal·lar aplicacions descarregades directament de P2P o de fòrums. Es corre el risc seriós que aquests programes continguen algun troià i, després de la instal·lació, infecten el dispositiu.

2.2.2 Desbloqueig/*root*

Els termes desbloqueig o arrel (*jailbreak/root*) d'un dispositiu es refereixen a concedir privilegis d'administració a les aplicacions saltant la barrera de protecció que tenen per defecte els sistemes operatius.

Aquesta característica pot afegir funcionalitats extra al dispositiu, però també és un risc extra al qual s'exposa, ja que s'elimina la barrera de protecció que sense desbloqueig o arrel es manté.

Llevat que siga absolutament necessari per al funcionament d'una aplicació concreta, es desaconsella habilitar aquesta característica en els dispositius.

2.2.3 Només les aplicacions necessàries

Omplir el dispositiu d'aplicacions innecessàries no sols n'alenteix el funcionament, sinó que augmenta el risc que una d'aquestes aplicacions tinga una vulnerabilitat que puga ser aprofitada per un atacant i aconseguir el control del dispositiu.

Per això és recomanable desinstal·lar qualsevol aplicació que no siga estrictament necessària per al funcionament del dispositiu, i així minimitzar el risc d'exposició per una aplicació vulnerable. A més, és important llegir els permisos i les condicions que cal acceptar abans d'instal·lar una aplicació i comprovar-ne la reputació.

2.2.4 Protecció antivirus

Es recomana disposar d'un antivirus en el dispositiu mòbil com a mesura extra de protecció contra el programari maliciós. En aquesta pàgina[8] es poden trobar diferents antivirus, molts dels quals estan disponibles també per a dispositius mòbils.

2.2.5 Actualitzacions de programari

Els sistemes operatius dels dispositius inclouen un sistema d'actualització d'aplicacions. Mitjançant una notificació, informen que hi ha una nova versió d'una aplicació instal·lada. Aquestes actualitzacions, a més d'afegir funcionalitats, corregeixen fallades de seguretat.

Sempre que el sistema notifique una actualització disponible, **s'ha d'acceptar i aplicar la nova versió**. Mantenint el sistema actualitzat s'eviten possibles infeccions per aplicacions vulnerables.

8 https://www.osi.es/es/herramientas-gratuitas?combine=&herramienta_selec%5B%5D=124&herramienta_selec%5B%5D=115

2.2.5.1 Actualitzacions programari Android

Per a comprovar que el nostre sistema està actualitzat s'ha de navegar fins a **Configuració/Quant al telèfon/Actualitzador d'aplicacions del sistema** i es verificarà que està marcada l'opció de Comprovació programada o Actualitzacions automàtiques.

Es pot comprovar de manera manual si es fa clic en **Comprova ara** o **Descàrrega manual** si el nostre sistema està completament actualitzat.

2.2.5.2 Actualitzacions programari iOS

En **Configuració/General/Actualització de programari** s'ha d'obtindre el missatge "El programari està actualitzat".

2.3 Altres de recomanacions

2.3.1 No emmagatzemar informació sensible

La informació més delicada de l'empresa o organització no ha de ser emmagatzemada en dispositius mòbils encara que estiga encriptada perquè els dispositius mòbils suposen riscos majors. Si s'ha d'accedir a aquesta informació crítica des d'un dispositiu mòbil, **ha de fer-se en línia a servidors segurs**.

2.3.2 Wi-Fi públiques

Les xarxes sense fils d'ús públic, o compartit, com les disponibles en hotels o cafeteries, poden suposar un risc. A pesar que tinga contrasenya per a poder utilitzar-la, un atacant podria connectar-s'hi i capturar el tràfic de totes les persones que es troben connectades a aquesta xarxa sense fil. Podria aleshores analitzar el trànsit capturat i recopilar contrasenyes o dades confidencials.

Si es vol utilitzar xarxes sense fils d'ús públic, es recomana no accedir a cap servei que requerisca contrasenya, realitzar operacions bancàries o descarregar documents confidencials.

2.3.3 Desactivar comunicacions sense fils

És molt important **desactivar les xarxes sense fils si no s'utilitzaran** a curt termini. Les xarxes més usuals solen ser Wi-Fi, Bluetooth o infrarojos. És possible fer atacs contra xarxes sense fils utilitzant punts d'accés falsos i enganyant el dispositiu perquè es connecte automàticament a una xarxa suposadament de confiança. L'usuari navegaria aleshores sense tindre constància que el trànsit està sent monitorat per un atacant.

A continuació, s'indica com desactivar el Bluetooth.

2.3.3.1 Desactivar Bluetooth. Android

En **Configuració/Bluetooth** es pot desactivar l'opció per a la connexió a través de Bluetooth. Es recomana **activar-lo únicament quan siga estrictament necessari.**

2.3.3.2 Desactivar Bluetooth. iOS

En la pantalla d'inici s'ha de fer clic en l'**Àrea de connexions** situada a la part superior de la pantalla i en la icona **Gestionar connexions**. Per a desactivar el Bluetooth cal **desmarcar la casella de verificació Bluetooth**.

2.3.4 Carregadors públics

S'han donat casos de **fugues d'informació** en dispositius mòbils per haver sigut connectats en **carregadors públics**.

S'ha d'evitar connectar el dispositiu per USB en qualsevol ordinador públic, com ara hotels o cibercafés, i qualsevol altre aparell que no ens genere confiança total. Ja que pot haver sigut manipulat per a extraure informació de qualsevol dispositiu USB que s'hi connecte.

2.4 Conclusions

L'ús tan estés de **dispositius mòbils** ha fet que es convertisquen de manera activa en una eina més del nostre treball, ja que allotgen en moltes ocasions informació corporativa crítica o valuosa que, en cas de ser interceptada, comportaria grans problemes de seguretat.

Aquest ús tan estés d'aquests dispositius ha fet que els ciberdelinqüents el vegen com un nínxol de mercat a explotar, i **hui dia, els dispositius mòbils s'han convertit en un dels focus principals davant d'atacs informàtics**. És per tot això que, tant els usuaris finals com les empreses han de posar tots els mitjans de què disposen per a implantar una estratègia de seguretat en mobilitat amb l'objectiu de garantir la integritat, confidencialitat i disponibilitat de la informació corporativa.

És important conéixer bé les opcions que cada fabricant ens ofereix, i aplicar una configuració de seguretat adequada per tal de **blindar el dispositiu mòbil sense perdre prestacions**.

També és **important saber** quina informació **podem emmagatzemar o no en el nostre dispositiu** (cal evitar sempre informació confidencial) i quines aplicacions (les mínimes i necessàries) i d'on les instal·lem (sempre de fonts fiables).

En definitiva, s'insta les empreses que establisquen **criteris i procediments adequats** per a implantar una estratègia de seguretat en mobilitat que comporte sobretot una correcta **formació i conscienciació** tant d'**usuaris com d'administradors**.

3. Contacte i consultes

Si es vol ampliar la informació sobre aquest o altres temes, o accedir a tota l'oferta formativa del Centre de Seguretat TIC de la Comunitat Valenciana, és possible fer-ho en els enllaços següents:

https://www.csirtcv.gva.es/?lang=va
https://www.facebook.com/csirtcv
https://twitter.com/csirtcv