DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Butlletí protecció de dades

Butlletí del Departament de protecció de dades i Seguretat de la Informació de la Diputació Provincial de València

Butlletí Nº 24| Juny 2022

SEGURETAT EN DISPOSITIUS MÒBILS

ÍNDEX

SEGURETAT EN DISPOSITIUS MÒBILS

Us convidem a traslladar-nos aquelles temàtiques que resultin del vostre interès per als propers butlletins informatius. Aquestes peticions s' hauran d' adreçar a:

Diputació de València

Departament de Protecció de Dades i Seguretat de la Informació

Pl. de Manises, 4 46003 València

email: dpdsi@dival.es

SUBSCRIPCIONS

Si desitges subscriure't al nostre Butlletí informatiu accedeix al següent enllaç

INTRODUCCIÓ

Es considera **dispositiu mòbil** al dispositiu electrònic d'ús personal o professional de reduïda grandària que permet la gestió (emmagatzematge, intercanvi i processament) d'informació i l'accés a xarxes de comunicacions i serveis remots, tant de veu com de dades, i que habitualment disposa de capacitats de telefonia, com per exemple telèfons mòbils, *smartphones* (telèfons mòbils avançats o intel·ligents), *tablets* (tauletes) i agendes electròniques, amb independència de si disposen de teclat físic o pantalla tàctil.

En els últims anys, el desenvolupament d' aquests dispositius, juntament amb les tecnologies sense fil, ha revolucionat la forma de treballar i comunicar-se, situant-los com un dels objectius principals per als atacants. Això fa necessari plantejar-se quina és la seguretat oferta per aquest tipus de dispositius respecte a la informació que gestionen, en especial dins dels entorns corporatius.

El present butlletí té com a objectiu ajudar als usuaris dels sistemes d'informació de la Diputació de València que per al desenvolupament de les seves tasques comptin amb dispositius mòbils, a fer un ús segur d'aquests. Per a això, s'oferiran un conjunt de recomanacions de seguretat per evitar o, si s'escau, mitigar possibles accions danyoses.

"EL DESENVOLUPAMENT DELS DISPOSITIUS MÒBILS, JUNTAMENT AMB LES TECNOLOGIES SENSE FIL, HA REVOLUCIONAT LA FORMA DE TREBALLAR I COMUNICAR-SE, SITUANT-LOS COM UN DELS OBJECTIUS PRINCIPALS PER ALS ATACANTS".

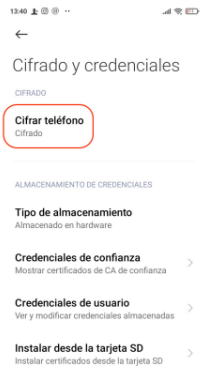
BONES PRÀCTIQUES EN LA CONFIGURACIÓ I ÚS DE DISPOSITIUS MÒBILS

HABILITAR LA PANTALLA DE BLOQUEIG

Els dispositius mòbils moderns resulten molt atractius per a la seva sostracció o robatori degut tant al seu valor econòmic, com al valor associat a la informació que emmagatzemen. La pantalla de bloqueig és el principal mecanisme de defensa davant l'accés físic no autoritzat al dispositiu mòbil per part d'un potencial atacant. L'objectiu que el dispositiu mòbil estigui exposat el menor temps possible davant accessos no autoritzats, fins i tot temporals, es recomana **configurar-lo perquè el codi d'accés sigui sol·licitat immediatament després d'apagar-se la pantalla**, que s'hauria de bloquejar automàticament al més aviat possible si no hi ha activitat per part de l'usuari (per exemple, després d'un minut).

No obstant això, fins i tot bloquejat el dispositiu mòbil, hi ha la possibilitat d'accedir a nombroses funcionalitats, com per exemple rebre i respondre missatges o trucades de telèfon, rebre notificacions d'esdeveniments i recordatoris, accedir a la càmera, modificar alguns ajustos, tenir accés a informació d'aplicacions (*app*) concretes, etc. Això també podria tenir implicacions en matèria de seguretat, per la qual cosa es recomana **limitar el màxim possible les funcionalitats disponibles en la pantalla de bloqueig si no s'introdueix el codi d'accés.**

XIFRAR EL DISPOSITIU

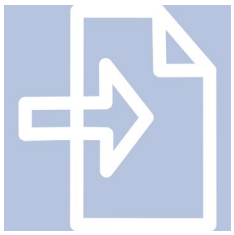


Les capacitats que permeten xifrar la memòria del dispositiu mòbil són imprescindibles davant l'accés físic no autoritzat al mateix per part d' un tercer, ja que, en cas contrari, seria possible extreure el contingut del xip de memòria del dispositiu mòbil i tenir accés a tota la informació emmagatzemada.

Si recomana **fer ús de les capacitats natives de xifrat del dispositiu mòbil,** amb l' objectiu de protegir totes les dades i informació associades a l' usuari o organització emmagatzemats en el mateix.

En cas que el dispositiu mòbil disposi d'una ranura per a una **unitat d' emmagatzematge externa**, normalment basada en la utilització de targetes de memòria SD, es recomana fer ús de capacitats de xifrat que permetin protegir també els continguts d' aquesta unitat externa d' emmagatzematge. En moltes ocasions no és possible xifrar aquests continguts, per la qual cosa **es recomana no emmagatzemar cap dada o informació sensible a la targeta SD, com per exemple documents corporatius.**

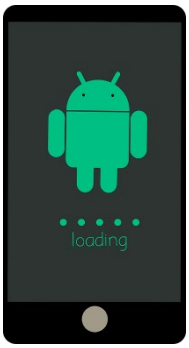
REALITZAR CÒPIES DE SEGURETAT



La protecció de la informació i les dades emmagatzemades i gestionades pel dispositiu mòbil s'ha d'estendre davant d'escenaris de pèrdua o robatori del mateix, així com davant danys en el *hardware* que no permetin accedir als continguts existents en la seva unitat d'emmagatzematge principal (o en les unitats externes).

Per evitar la pèrdua de les dades, l'usuari ha **de realitzar còpies de seguretat (*backups*) periòdiques, i preferiblement automàtiques**, de tots els continguts del dispositiu mòbil que es vol protegir i conservar.

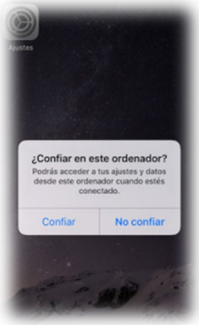
ACTUALITZAR EL SISTEMA OPERATIU I LES APLICACIONS



Els dispositius mòbils disposen d'un sistema operatiu mòbil (*Android, iOS*, etc.), també denominat *firmware*, que proporciona totes les funcionalitats per defecte, i que també inclou un conjunt d'aplicacions mòbils que han estat instal·lades pel fabricant del sistema operatiu, del dispositiu o de l'operador de telecomunicacions.

Es recomana **tenir el sistema operatiu sempre actualitzat en el dispositiu mòbil**. Així mateix, es recomana **disposar sempre de l'última actualització de totes les *apps* instal·lades en el dispositiu mòbil**. L'última versió tant del sistema operatiu com de les *apps* **soluciona vulnerabilitats públicament conegudes** i, per tant, redueix significativament l'exposició del dispositiu davant d'atacs.

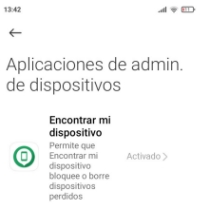
COMPTE AMB LES CONNEXIONS A TRAVÉS D' USB



Els ports de càrrega i sincronització dels dispositius mòbils permeten la connexió per fil mitjançant un port USB a un ordinador o endoll. Això permet, d' una banda, la transmissió d'energia elèctrica per dur a terme la càrrega de la bateria del dispositiu mòbil, i de l'altra, establir comunicacions de dades. Els atacants han emprat aquesta funcionalitat dual per comprometre els dispositius mòbils a través de la connexió de dades, fent-se passar per una estació de càrrega en llocs públics. Mitjançant aquest atac és possible extreure dades personals emmagatzemades en el dispositiu mòbil, així com dur a terme accions més danyoses, com la instal·lació d'apps danyoses.

Es recomana **no connectar el dispositiu mòbil a ports USB desconeguts i no acceptar cap relació de confiança si no es té constància d'estar connectant el dispositiu mòbil a un ordinador de confiança**.

GESTIÓ REMOTA DEL DISPOSITIU MÒBIL



Els dispositius mòbils moderns permeten a qualsevol usuari localitzar la ubicació actual del seu dispositiu mòbil, bloquejar-lo en cas de trobar-se desbloquejat, fer que soni per identificar la seva ubicació propera, eliminar remotament les dades emmagatzemades en el mateix, etc.

Es recomana a l' usuari **familiaritzar-se amb les capacitats de gestió remota del dispositiu mòbil** i la seva plataforma mòbil associada, i **comprovar el correcte funcionament** d' aquest servei i de tota la seva funcionalitat abans que sigui necessari fer-ne ús en un escenari real després de la pèrdua o robatori del dispositiu mòbil.

CONNEXIÓ A XARXES WI-FI

L'interfície Wi-Fi és probablement el mecanisme de comunicació més utilitzat en l'actualitat en els dispositius mòbils a l'hora d'intercanviar dades i accedir a serveis i aplicacions remotes.

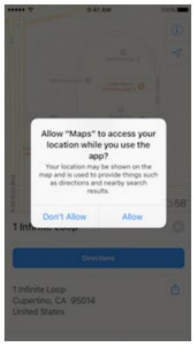
Si recomana **no connectar el dispositiu mòbil a xarxes Wi-Fi públiques obertes** que no implementen cap tipus de seguretat. Encara que la seva utilització no tingui cap cost associat, s'està posant en risc la informació personal de l'usuari. La utilització d'aquestes xarxes permet a un potencial atacant interceptar i manipular tot el trànsit intercanviat pel dispositiu mòbil.

COMPTE AMB LES APLICACIONS MÒBILS QUE ES DESCARREGUEN

Els dispositius mòbils com els *smartphones* són considerats intel·ligents perquè, entre altres motius, disposen de la capacitat d'estendre les funcionalitats existents per defecte mitjançant la instal·lació de noves aplicacions mòbils (*apps*).

Es recomana **no instal·lar cap app que no sigui estrictament necessària per al desenvolupament de les tasques encomanades en l'organització** i, en cas de descarregarla, que provingui **d'una font de confiança, com per exemple els mercats oficials *d'apps*.** Tot i que s'han donat diversos casos de codi danyós botigues oficials, els controls existents fan que la probabilitat d'infecció sigui menor que en altres plataformes mòbils, i un cop detectat, és eliminat del mercat al més aviat possible.

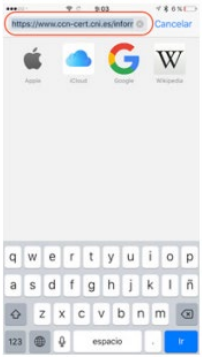
ADEQUADA GESTIÓ DELS PERMISOS DE LES *APPS*



Per obtenir accés a funcionalitats addicionals, las *apps* demanen sovint permisos a l'usuari, per exemple, per accedir als seus contactes, al seu calendari, a components *hardware* del dispositiu mòbil, com la càmera o el micròfon o a les fotos. Els permisos se sol·liciten a l'usuari en el moment de la instal·lació de l'app o durant la seva execució, en el moment de fer ús de certa funcionalitat per a la qual un permís concret sigui necessari.

Es recomana **no atorgar permisos innecessaris o excessius** a les apps, limitant així les dades i la funcionalitat a la qual aquestes tindran accés. Per a això, és necessari que prèviament l'usuari entengui per què una app demana un permís determinat i per a què és necessari aquest permís dins de la funcionalitat proporcionada per *l'app*.

NAVEGACIÓ WEB SEGURA



Es molt habitual que els dispositius mòbils siguin utilitzats per a tasques de navegació web.

Es recomana, sempre que sigui possible, **fer ús del protocol HTTPS** mitjançant la inserció del text "https://" abans d'introduir l'adreça web del servidor amb el qual es vol connectar.

Desafortunadament, per defecte, la barra de direcció dels navegadors web dels dispositius mòbils moderns tendeix a minimitzar la informació mostrada a l'usuari, destacant únicament el domini amb el qual s'ha establert la connexió. Per poder obtenir tots els detalls del servidor web i del recurs accedit, així com verificar si el mètode de connexió emprat és HTTPS (verificar que apareix un candau no sempre és suficient), pot ser necessari seleccionar la barra de direcció i desplaçar-se cap a l'esquerra per visualitzar tots els detalls.

ESPECIAL CURA AMB EL CORREU, SMS I SERVEIS DE MISSATGERIA

A través d'aquests serveis és possible rebre missatges amb enllaços web o adjunts que alberguen codi danyós, amb l'objectiu d'infectar i comprometre el dispositiu mòbil de l'usuari víctima. L'ús d'enllaços danyosos és una de les tècniques més utilitzades per aconseguir executar codi en el dispositiu mòbil de la víctima o bé per obtenir-ne informació.

Els atacs basats en enllaços maliciosos distribuïts a través de les *apps* de

missatgeria se solen referenciar com *SMiShing*, i també inclouen missatges atractius, suggerents o sobre els quals l'usuari hauria de dur a terme una acció urgent.

El consell més eficaç per identificar missatges danyosos és el **sentit comú.** Això significa que **qualsevol símptoma o patró fora del considerat normal o habitual ha de despertar la sospita de l'usuari**. Un patró o símptoma irregular pot significar: rebre un missatge d'un remitent no conegut, rebre un missatge que demani informació personal, que el contingut del missatge sigui massa atractiu com per a ser cert, etc.

DEURE D' INFORMAR EN CAS D' INCIDENT RELACIONAT AMB EL DISPOSITIU

S'ha **d'informar immediatament el responsable de seguretat de l'organització** en el cas de perdre o extraviar el dispositiu mòbil, igual que si s' identifica qualsevol comportament anòmal o sospitós en fer-ne ús.

"LA CONSCIENCIACIÓ, EL SENTIT COMÚ I LES BONES PRÀCTIQUES EN LA CONFIGURACIÓ I L'ÚS DELS DISPOSITIUS MÒBILS CONSTITUEIXEN LA MILLOR DEFENSA PER PREVENIR I DETECTAR AQUEST TIPUS D' INCIDENTS I AMENACES".

MATERIAL COMPLEMENTARI

- Informe: *"Dispositivos móviles. Informe de buenas prácticas"* (CCN). Consulta l' informe en aquest enllaç.
- Guia: *"Privacidad y Seguridad en Internet"* (AEPD). Consulta la Guia en aquest enllaç.
- "¿Trabajas desde tu dispositivo móvil? ¡Implementa las mismas medidas de seguridad que en tu oficina!" (INCIBE). Consulta el post en aquest enllaç.
- *"Cómo prevenir incidentes en los que intervienen dispositivos móviles"* (INCIBE). Consulta el post en aquest enllaç.
- *"Decálogo de buenas prácticas en seguridad móvil"* (INCIBE). Consulta el post en aquest enllaç.
- Guía: *"Dispositivos móviles personales para uso profesional (BYOD)"* (INCIBE). Consulta la Guia en aquest enllaç.
- Política: *"Uso de dispositivos móviles no corporativos"* (INCIBE). Consulta aquest enllaç.
- Dossier: *"Protección en movilidad y conexiones inalámbricas"* (INCIBE). Consulta el dossier en aquest enllaç.
- *"Protege tu móvil iOS y Android con 5 consejos"* (OSI). Consulta aquest enllaç.

NOTÍCIES

- **Es publica Real Decreto 311/2022, de 3 de mayo, por el que se regula el nuevo Esquema Nacional de Seguridad (ENS).**

  El nou ENS no pretén ser un canvi disruptiu, sinó que té cert caràcter continuista però actualitzat. Aquesta actualització se centra en alguns pilars fonamentals: alinear l'ENS amb el nou marc normatiu de referència; introduir la capacitat d'ajustar els requisits de l'ENS a necessitats específiques, determinats col·lectius o determinats àmbits tecnològics; actualitzar els principis bàsics, els requisits mínims i les mesures de seguretat; perfeccionar el capítol de "Prevenció, detecció i resposta a incidents de seguretat"; en general, clarificar, precisar, homogeneïtzar, simplificar i actualitzar diferents aspectes. Destaca la inclusió de la professionalització dels rols a qui correspon vetllar per la seguretat de la informació, igual que el Reglament Europeu de Protecció de Dades introdueix la figura del Delegat de Protecció de Dades. És a dir, s'exigeix la formació, qualificació i dedicació d'aquests rols.

  Consulta la norma en aquest enllaç.
  Consulta les infografies publicades pel CCN en aquest enllaç.

- **Nova secció sobre salut i protecció de dades al web de l' AEPD.**

  La nova secció està composta per set apartats que recullen des d'informació general sobre el tractament de les dades de salut i com exercir el dret d'accés a la història clínica a qüestions relacionades amb la investigació mèdica o les bretxes de dades personals.

  Consulta aquest enllaç.