



Butlletí

Protecció de dades

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

Butlletí N.º 39 | Setembre 2023

RECOMANACIONS DE SEGURETAT EN INTERNET



ÍNDEX



RECOMANACIONS DE SEGURETAT EN INTERNET

INTRODUCCIÓ	2
RECOMANACIONS DE SEGURETAT EN INTERNET	3
NOTÍCIES	13



Us convidem a traslladar-nos aquelles temàtiques que resulten del vostre interès per als pròxims butlletins informatius. Aquestes peticions hauran de dirigir-se 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's al nostre Butlletí informatiu accedeix al següent [enllaç](#)



INTRODUCCIÓ



Internet i els serveis que a través d'ella es presten s'han convertit en un element imprescindible per a les nostres vides.

A més, l'explosió de la connectivitat mitjançant l'ús massiu de dispositius mòbils intel·ligents, especialment, els *telèfons intel·ligents*, i xarxes de dades mòbils cada vegada més ràpides, fa que tots aquests serveis es puguin consumir en qualsevol lloc i a qualsevol hora del dia o de la nit, per la qual cosa podem parlar de "*persones connectades*" més que de dispositius i ordinadors connectats.

Els serveis més usats en la xarxa es presten gràcies a la quantitat d'informació i dades personals que els usuaris aportem, tant a les empreses que ofereixen els serveis com a altres usuaris, per la qual cosa hem de ser conscients dels riscos que això pot suposar per a la nostra seguretat i privacitat.

L'objectiu d'aquest butlletí és promoure l'ús segur i responsable d'Internet, explicant els riscos als quals estem exposats i proporcionant les pautes necessàries per a traure partit als serveis sense comprometre la nostra seguretat i privacitat. D'aquesta manera, ens servirà també de conscienciació per a l'ús d'Internet en el nostre centre de treball, els quals, cada vegada són més objectiu de la ciberdelinqüència.



RECOMANACIONS DE SEGURETAT EN INTERNET

1. EMMAGATZEMATGE DE INFORMACIÓ PRIVADA EN DISPOSITIUS

Un dels principals motius per a protegir els nostres dispositius mòbils és salvaguardar la nostra informació personal i la d'aquelles persones amb les quals ens comuniquem: contactes, fotografies, vídeos, correus electrònics, etc.



CONSELLS I RECOMANACIONS

El risc de pèrdua o robatori sempre existirà, per tant, tingues en compte les següents recomanacions:

- Utilitza un mètode de bloqueig de la pantalla (codi numèric o patró) i xifra la informació perquè, si aquesta situació es produeix, dificultes l'accés a la persona que acabe amb el dispositiu a les seues mans.
- Fes ús d'eines de seguretat que t'ajudaran a localitzar el dispositiu, bloquejar-lo i fins i tot eliminar la informació emmagatzemada en ell.
- Realitza còpies de seguretat en un altre suport perquè, passe el que passe, no perdes la informació emmagatzemada en el mòbil o tauleta.

En el dispositiu, només disposa d'aplicacions segures:

- Descarrega únicament a través de les botigues d'aplicacions (apps) oficials.
- Revisa prèviament la valoració i els comentaris que els usuaris han fet sobre una determinada app. Quan es comporta malament o de manera sospitosa, els propis usuaris s'encarreguen de reflectir-ho en els comentaris.
- Instal·la una eina antivirus perquè detecte possibles apps malicioses que intenten colar-se en el teu dispositiu.

En el cas de les xarxes wifi públiques a les quals ens connectem, és recomanable que:

- No intercanvies informació privada o confidencial.
- No et connectes al servei de banca on-line.
- No realitzes compres

2. PER QUÈ SÓN TAN IMPORTANTS LES CONTRASENYES?

És molt comú utilitzar la mateixa contrasenya per a accedir a diferents serveis, si en algun moment la teua contrasenya es vera compromesa, el risc per a la teua informació personal seria molt major, ja que no sols podrien accedir a un dels teus serveis sinó a tots aquells en els quals utilitzares la mateixa clau per a accedir.

Hem d'usar contrasenyes fortes i protegir-les. Les contrasenyes són les claus que donen accés als teus serveis i per tant a la teua informació personal, per la qual cosa si algú les aconsegueix podria comprometre la teua privacitat.

CONSELLS I RECOMANACIONS

Tria contrasenyes fortes o robustes d'almenys 8 caràcters i composta per:

- Majúscules (A, B, C...)
- Minúscules (a, b, c...)
- Números (1, 2, 3...)
- I caràcters especials (\$, &, #...)
- No utilitzes contrasenyes fàcils d'endevinar com: "12345678", "qwerty", "aaaaa", noms de familiars, matrícules de vehicles, etc.
- No compartisques les teues contrasenyes. Si ho fas, deixarà de ser secreta i estaràs donant accés a altres persones a la teua privacitat.
- No uses la mateixa contrasenya en diversos serveis.



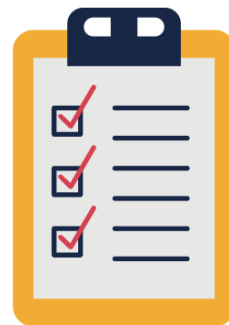
Quan maneges moltes contrasenyes i no eres capaç de recordar-les totes, utilitza un gestor de contrasenyes. És un programa que et permet emmagatzemar de manera segura les teues claus d'accés als diferents serveis.

Només necessites recordar la clau d'accés al gestor de contrasenyes, coneguda com a clau mestra, per a consultar la resta de les teues contrasenyes.

Malgrat el fort o robusta que siga la teua contrasenya, amb el pas del temps pot veure's compromesa; canvia les teues contrasenyes periòdicament.

3. SÓN SUFICIENTS LES CONTRASENYES?

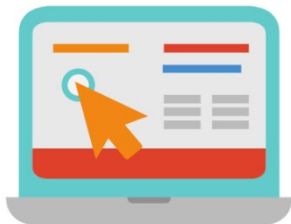
La seguretat d'un servei protegit únicament per una contrasenya depén exclusivament d'aquesta, això implica un risc de seguretat ja que, si algú l'obtinguera sota alguna circumstància, no sols tindria accés al teu compte d'usuari, sinó que també podria realitzar activitats fraudulentas en el teu nom o tafanejar la teua informació personal.



CONSELLS I RECOMANACIONS

- Una manera de protegir un compte d'usuari és fent ús de sistemes de verificació en dos passos que consisteixen a afegir una capa de seguretat extra al procés de registre/login d'un determinat servei en línia, és a dir, per a accedir a ell, a més d'un nom d'usuari i una contrasenya, serà necessari que facilites un codi que només tu coneixes i que generalment s'obté a través del dispositiu mòbil.
- Ací, es dificulta l'accés a tercers persones als teus serveis en línia, ja que, encara que aconseguisquen per algun mètode la teua contrasenya, necessitaran també introduir un codi que només podran conèixer si disposen físicament del teu telèfon mòbil.
- Depenent del servei, podràs usar un mètode o un altre, actualment el més habitual és l'enviament d'un codi a través d'un missatge SMS a un número de telèfon prèviament configurat. Una vegada rebut aquest codi, cal introduir-ho com un segon pas addicional abans d'aconseguir accedir al servei.
- Si tens identificats dispositius de confiança no tindràs que ficar el codi cada vegada que vulgues accedir a un determinat servei. Marcant-ho com a tal, només puntualment hauràs d'introduir-ho, fent que la doble verificació resulte una tasca més àgil.
- Alguns serveis fins i tot no disposen d'opcions de verificació en dos passos. Si et trobes en aquesta situació, assegura't d'usar contrasenyes robustes i gestiona aquestes adequadament per a evitar problemes de seguretat i privacitat.

4. FIABILITAT EN LES PÀGINES WEBS



El desconeixement d'uns certs aspectes de seguretat provoca que cometes errors, pugues ser víctima d'algun frau o simplement no faces res per por. Però, a continuació, s'aporten una sèrie de consells i recomanacions.

CONSELLS I RECOMANACIONS

El primer que s'ha de fer és assegurar que el teu dispositiu està preparat per a realitzar els diferents tràmits, per a això:



- Instal·la un antivirus i manteniu-lo actualitzat perquè detecte les últimes amenaces que circulen per la xarxa.
- El teu equip i els seus programes, com el navegador, també tenen que estar actualitzats i correctament configurats.
- Crea un compte d'usuari per cada persona que vaja a utilitzar el dispositiu.
- La connexió és important, sempre que vages a realitzar tràmits en línia evita fer-ho des de xarxes wifi-públiques. Connecta't millor amb el 3G/4G del mòbil o des del teu wifi de casa i no t'oblides de comprovar si la teua xarxa wifi està correctament configurada per a evitar que desconeguts es connecten a ella.
- Quan visites un lloc, comprova que realment és al qual volies accedir. Fixa't en la URL, aquesta començarà per https i mostrarà un cadenat en la barra d'adreces. Quan faces clic sobre aquest cadenat, la URL també haurà d'estar ben escrita.
- Quan acabes, no t'oblides de tancar la sessió. Prem sobre l'opció de tancar sessió en finalitzar. Si no ho fas, la teua sessió quedarà oberta i les teues dades personals i/o bancaries estaran visibles per a les persones que utilitzen el mateix dispositiu per a connectar-se a Internet.

Altres recomanacions útils en diferents àmbits:

Gestions amb la teua banca en línia o l'administració pública

- Mantingues en secret les teues contrasenyes d'accés. No les guardes escrites ni les compartisques amb ningú.
- No respongues mai a correus que et sol·liciten les teues dades personals i/o bancaris.



- Davant qualsevol dubte, contacta directament amb el banc o el servei públic per a solucionar el problema.

Compres en línea:

- Comprova si el preu mostrat és el final o si cal sumar-li altres impostos o càrrecs addicionals.
- Esbrina les formes de pagament permeses.
- Consulta les opinions que altres usuaris tenen sobre la pàgina web o el venedor mitjançant cerques en la xarxa.
- Revisa les condicions d'enviament i identifica la política de devolucions.

5. COM PUC USAR EL NAVEGADOR PERQUÈ NO EMMAGATZEME TOTS ELS PASSOS QUE DONE PER INTERNET?



Quan navegues per Internet, per defecte tota l'activitat que has realitzat amb el navegador s'emmagatzema directament en la memòria del teu ordinador o dispositiu, no desapareix. De tal forma que, és possible saber tots els passos que vas donar en un moment donat per Internet. Per a evitar això, i especialment si fas ús de dispositius públics o compartits amb altres persones, els navegadors incorporen l'opció de "navegació privada".

Has de saber quina informació manegen els navegadors sobre tu i quines opcions incorporen perquè pugues gestionar-la adequadament, és important per a poder evitar riscos com:

- Que tota la teua activitat en Internet estiga exposada a qualsevol persona que tinga accés al navegador.
- Donar pistes sobre el teu comportament i preferències en la Xarxa.
- Que la teua sessió en un lloc web quede oberta en el navegador i suplanten la teua identitat.

La navegació privada evita que altres persones sàpien les pàgines que has visitat, els productes que has adquirit, la publicitat que t'ha interessat, etc.

CONSELLS I RECOMANACIONS

Independent del navegador que utilitzes, és necessari que adoptes una sèrie de mesures per a minimitzar els riscos als quals t'exposes quan l'uses per a navegar per Internet. Per tant:

- Mantingues el navegador actualitzat a l'última versió.
- Tria complements i plugins de confiança, descarrega'ls només de llocs coneguts i amb bona reputació com són les pàgines oficials dels navegadors.
- Instal·la un verificador de pàgines web, normalment proporcionat pels principals antivirus.
- Revisa les opcions de configuració del navegador i habilita aquelles que consideres més interessants per a protegir la teua privacitat i mantindre't més segur.
- Esborra l'historial de navegació quan no el necessites.
- Elimina les cookies, aqueixos xicotets fitxers que guarden informació dels llocs que visites.



- Utilitza un gestor de contrasenyes per a emmagatzemar i custodiar les teues claus d'accés i evitar així utilitzar els teus navegadors com a gestors de contrasenyes.
- Tanca sempre la sessió quan isques d'una pàgina en la qual t'hages autenticat amb usuari i contrasenya. Amb aquesta acció evites que si una persona utilitza el teu ordinador o el teu dispositiu mòbil pugua accedir a la teua informació personal usant la sessió que has deixat oberta.



6. QUI POT VEURE EL QUE PUBLIQUE EN UNA XARXA SOCIAL?

CONSELLS I RECOMANACIONS

Quan et registres, algunes xarxes socials et sol·licitaran moltes dades sobre tu: domicili, lloc de treball, col·legi, gustos, aficions, familiars, etc., que no són obligatoris. Valora quina informació personal vols proporcionar.

Hi ha cert tipus d'informació que no hauries de publicar en els teus perfils perquè no comprometa la teua privacitat ni siga utilitzada:

- Dades personals
- Contrasenyes
- Dades bancàries
- Telèfon mòbil
- Plans per a les vacances
- Comportaments inapropiats
- Ideologies
- Dades mèdiques o relatives a la teua salut



A més, amb el pas dels anys, la informació que publiqués en Internet es converteix en la teua reputació digital.

Revisa les opcions de configuració de cada xarxa social per a tindre controlats els principals aspectes de privacitat i seguretat:

- Conèixer qui té accés a les teues publicacions
- Saber qui et pot etiquetar
- Si el teu perfil està visible als cercadors d'Internet
- Conèixer la geolocalització de les publicacions, etc.

7. RISCOS EN SERVEIS DE MENSAJERIA INSTANTÀNIA

Conèixer les estratègies d'engany que utilitzen els ciberdelinqüents et pot ajudar a evitar caure en els seus parany, solen utilitzar alguns d'aquests mètodes:



- Missatges de contactes desconeguts
- Enllaços a pàgines web que no coneixes on et redirigeixen, molt menys si es tracta d'un enllaç acurtat.
- Faules i missatges en cadena. No els reenvies.
- Contrasta la informació i assegura't que és veraç. Posa especial atenció si el missatge en aquells casos en què puga sonar alarmista, (si no fas el que et demanen passarà alguna cosa) o se sol·licita informació privada (dades personals, bancaris, de domicili...) o conté premis i cupons o sortejos, els quals abans ha d'emplenar una enquesta i/o realitzar la descàrrega d'alguna aplicació:

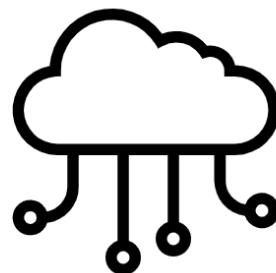
CONSELLS I RECOMANACIONS

- Foto de perfil: Cerca una que no siga molt compromesa.
- Bloqueig d'usuaris: Decideix amb qui vols mantindre comunicació i amb qui no.
- Informació d'estat: No utilitzes el teu estat per a facilitar informació privada sobre tu.
- Assegura't que l'intercanvi de missatges estiga xifrat, així, encara que algú els intercepte, no podrà comprendre'ls.
- Fes ús de l'opció de xat privat i/o secret i evita que persones alienes a la conversa puguen espiar-la.
- Realitza còpies de seguretat si no vols perdre els missatges de xat.

Les apps de missatgeria instantània en telèfons intel·ligents no solen demanar usuari i contrasenya cada vegada que les utilitzem. Això significa que, en cas de pèrdua o robatori, la persona que es faça amb el dispositiu podria enviar missatges a tots els contactes de la víctima fent-se passar per ella.

8. QUE CAL TINDRE EN COMPTE EN SERVEIS CLOUD

Els serveis d'emmagatzematge en el núvol et permeten accedir als teus fitxers des de qualsevol lloc i dispositiu, incloent-hi telèfon intel·ligent o tauleta, crear carpetes per a organitzar la informació i compartir arxius si ho necessites, entre altres. Fins i tot tens l'opció de seleccionar una carpeta del teu dispositiu que es sincronitze automàticament amb el servei en el núvol, generant d'aquesta manera una còpia de seguretat en línia de la informació. No obstant això, aquests avantatges es poden convertir en inconvenients si no prens les mesures de seguretat i privacitat adequades.



CONSELLS I REMENJANDACIONES

Tria les opcions i els serveis d'emmagatzematge que millor s'adapten a les teues necessitats, llig els seus termes i condicions d'ús abans d'acceptar-los i segueix aquests consells:

- Assegura't que l'accés al servei en el núvol siga baix HTTPS.
- Configura correctament les opcions de privacitat i seguretat que proporciona el servei.
- Per a major seguretat, xifra les teues dades més confidencials abans de pujar-les al servei del núvol.
- Utilitza una contrasenya robusta d'accés i no la compartisques.
- Fes còpies de seguretat en suports alternatius.
- Si comparteixes fitxers, assegura't que el destinatari és realment qui desitges.

“En la missatgeria instantània: Contrasta la informació i assegura't que és veraç. Posa especial atenció al missatge en aquells casos en què puga sonar alarmista, (si no fas el que et demanen passarà alguna cosa) o se sol·licita informació privada (dades personals, bancaris, de domicili...) o conté premis i cupons o sortejos, els quals abans ha d'emplenar una enquesta i/o realitzar la descàrrega d'alguna aplicació”.



MATERIAL COMPLEMENTARI

- Article tècnic sobre “Mesures per a minimitzar el seguiment en internet” (AEPD). Pots consultar l'article en [aquest enllaç](#).

Article Tècnic sobre “Accés d'aplicacions a la pantalla en dispositius Android” (AEPD).

Pots consultar l'article en [aquest enllaç](#).

- Article Tècnic sobre “Introducció a les tecnologies 5G i els seus riscos per a la privacitat” (AEPD). Pots consultar l'article en [aquest enllaç](#).
- Infografia sobre “10 Consells per a comprar en internet de manera segura” (AEPD). Pots consultar la infografia en [aquest enllaç](#).
- Infografia “Compra segura en Internet” (AEPD). Pots consultar l'article en [aquest enllaç](#).
- Infografia “Recomanacions per a l'ús segur de la internet de les coses” (AEPD). Pots consultar la infografia [aquest enllaç](#).

NOTÍCIES

- **La APDCAT emet una Recomanació en relació amb la contractació de la figura del Delegat de Protecció de Dades.** L'Autoritat Catalana de Protecció de Dades (APDCAT) ha publicat la Recomanació 2/2023, per a advertir a les entitats del seu àmbit d'actuació que cal tindre en compte la rellevància de funcions a desenvolupar a l'hora de fixar els preus del contracte dels serveis de delegat de protecció de dades personals (DPD). Això després de constatar licitacions en les quals s'ha tingut en compte exclusivament el factor preu i, fins i tot, s'ha establert un valor estimat del contracte notòriament baix en relació amb l'activitat a desenvolupar. Consulta la Recomanació en [aquest enllaç](#).
- **L'AEPD sanciona a la Conselleria d'Educació, Universitats, Cultura i Esports del Govern de Canàries (CEUCD) per vulnerar els articles 13, 6.1 i 32 del RGPD en l'ús de la plataforma educativa Google Suite.** L'IES va donar d'alta en la plataforma al fill menor d'edat del reclamant durant el curs 20/21 sense la seua autorització i amb anterioritat a la seua implantació per la CEUCD, la qual va tindre lloc en el curs 21/22 en el marc del Conveni signat per la Conselleria amb GOOGLE. A més, no s'acredita que s'haja facilitat tota la informació prevista en l'article 13 RGPD. Consulta la Resolució en [aquest enllaç](#).
- **L'AEPD sanciona a l'Ajuntament de Santiago de Compostel·la per la forma en la qual va remetre una notificació en la qual s'exposaven les dades d'un conductor en una denúncia per excés de velocitat.** El reclamant va rebre una carta sense sobre que va ser recollida per un familiar. Consulta la Resolució en [aquest enllaç](#).