

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 N.º 2 | Agost 2020

PLATAFORMES I APLICACIONS EN EL TELETREBALL



Í N D E X



	Pág
Tema central	
Plataformes y aplicacions en el teletraball	2-6
Material complementari	7
• Recomanacions de l'AEPD per a protegir les dades personals en situacions de mobilitat i teletreball .	
• Recomanacions de Seguretat per a situacions de teletreball i reforç en vigilància.	
• Avantprojecte de Llei de Treball a Distància.	
Notícies d'actualitat	7



Vos invitem a traslladar-nos aquelles temàtiques que resulten del vostre interès per als pròxims butlletins informatius. Estas peticions hauran de dirigir-se a:

Diputació de València

Dpt. de Protecció de Dades i
Seguretat de la Informació

Pl. de Manises, 4 46003 València

email: dpdssi@dival.es

SUBSCRIPCIONS

Si desitges subscriure's al nostre Butlletí informatiu accedix al següent

[enllaç](#)



PLATAFORMES Y APLICACIONES EN EL TELETREBALL

Pareix que el teletreball ha vingut per a quedar-se, no sols com a circumstància sobrevinguda ja que com indiquem en el butlletí anterior, des del Ministeri de Treball s'ha elaborat un avantprojecte de llei, presentat el passat 26 de juny, per a regular l'ocupació a distància. Algunes de les qüestions que aborda són la voluntarietat de triar esta forma de treballar, **el repartiment de costos, la desconexió digital o l'horari**, ocasionant que el mercat laboral a Espanya passa per impulsar definitivament la instauració del teletreball.

Amb motiu del canvi de perspectiva a què ens estem enfrontat, donada la impossibilitat de desenrotllar els servicis de forma presencial, ha sigut necessari adaptar la nostra metodologia de treball a un sistema digital. Per això, el present butlletí atén a la necessitat de busca d'alternatives per a continuar amb la prestació de l'activitat de manera efectiva, sense oblidar el compliment del marc jurídic que ha d'enquadrar-se en el desenrotllament de la nostra activitat.

Veurem algunes de les qüestions a tindre en compte perquè la **implementació d'un sistema digitalitzat es desenrotlle sense riscos jurídics, aclarint una sèrie d'aspectes que tant ocupador com empleat** deuen de tindre en compte per a establir una bona estratègia de teletreball.



Supòsits d'aplicació

El desenrotllament de l'adequada implementació del treball a través de modalitats a distància i online pot ser necessària per a:

- **Utilització d'aplicacions per a desenrotllar reunions** de forma telemàtica a través de videoconferència (Skype, Google Hangouts, Webex, Teams y Zoom)
- **Utilització de ferramentes d'emmagatzemament en núvol** (tipo Dropbox, Google Drive, OneDrive, etc.)
- Utilització de **correu electrònic** per a l'intercanvi d'informació entre treballadors



Tractament de dades personals en internet

Hui en dia hem vist que la necessitat d'atendre a situacions com la que ens trobem actualment, suposa que les entitats hagen recorregut a les solucions que faciliten les tecnologies de la informació i comunicació, en particular a l'ús de servicis de *cloud computing* o de computació en núvol i aplicacions per a desenrotllar reunions de forma telemàtica a través de videoconferència.

En estos supòsits és essencial atendre a les obligacions derivades de la normativa aplicable en matèria de protecció de dades, analitzant les implicacions que plantegen l'ús de les dites plataformes.

En este sentit, l'entitat haurà de disposar de la informació clarament definida sobre els tractaments efectuats, les finalitats dels mateixos i els seus responsables, així com sobre la ubicació de les dades, el període de retenció, i les garanties amb relació a la seua seguretat, que ofereixen les dites plataformes.

“L'ENTITAT HAURÀ DE DISPOSAR DE LA INFORMACIÓ CLARAMENT DEFINIDA SOBRE ELS TRACTAMENTS EFECTUATS, LES FINALITATS DELS MATEIXOS I ELS SEUS RESPONSABLES, AIXÍ COM SOBRE LA UBICACIÓ DE LES DADES, EL PERÍODE DE RETENCIÓ, I LES GARANTIES AMB RELACIÓ A LA SEUA SEGURETAT, QUE OFERIXEN LES DITES PLATAFORMES”

ORIENTACIONS PER A L'AVALUACIÓ D'APLICACIONS

Per a la pròpia entitat, les connexions remotes poden ser una via d'entrada de codi danyós als sistemes, per això, es considera clau poder garantir la seguretat d'estes connexions i accessos. Així, hem de garantir que els empleats coneguen una sèrie de bones pràctiques en l'exercici de les seues funcions:

A) Sobre la informació oferida pels responsables de l'aplicació

S'ha de comprovar si el responsable de l'aplicació informa clarament dels següents:

- la identitat i direcció del responsable,
- les finalitats per a les que seran utilitzats les dades,
- les possibles comunicacions de dades a tercers i la seua identitat, així com la finalitat per a la que se cedixen,
- els drets que assistixen als titulars dels dades,
- la ubicació de les dades i els seus períodes de conservació,
- les mesures de seguretat facilitades per l'aplicació,
- els possibles accessos que realitza l'aplicació a les dades personals emmagatzemats en el dispositiu o als seus sensors.



Esta informació hauria d'estar fàcilment accessible en la política de seguretat de l'aplicació. En el cas que falte algun d'estos aspectes, o que la informació facilitada no oferisca les garanties adequades, es recomana no utilitzar l'aplicació.

B) Sobre la ubicació de les dades

Les dades han d'estar emmagatzemats en un país de l'Espai Econòmic Europeu o un país que oferisca un nivell de protecció equivalent (que haja sigut així acordat per l'Agència Espanyola de Protecció de Dades o per Decisió de la Comissió Europea).

Pot consultar la llista de països amb nivell adequat de protecció en el següent enllaç.

En qualsevol altre cas, es recomana sol·licitar informació sobre les possibles transferències internacionals de dades i les garanties de la seua licitud, en particular sobre les quals necessiten autorització per part de l'Agència Espanyola de Protecció de Dades.

“LA RESPONSABILITAT DEL COMPLIMENT DE LES MESURES DE SEGURETAT HA D'ENTENDRE'S SEMPRE COMPARTIDA ENTRE ELS DIFERENTS ACTORS INTERVINENTS (RESPONSABLE DE L'APLICACIÓ, L'ENTITAT I ELS USUARIS)”

C) Sobre la seguretat dels dades

La responsabilitat del compliment de les mesures de seguretat ha d'entendre's sempre compartida entre els diferents actors intervinents (responsable de l'aplicació, l'entitat i els usuaris), devent en tot cas el responsable de l'aplicació facilitar les mesures tècniques adequades per a garantir la seguretat de les dades tractats, i l'entitat aplicar-les o utilitzar-les correctament, a més d'implementar les mesures organitzatives apropiades.

Així, per exemple, l'aplicació ha de proveir mecanismes que permeten la realització de còpies de seguretat o la descàrrega de les dades, de tal forma que l'entitat puga complir amb les obligacions que li són exigibles respecte d'això, introduint en la seua política de seguretat la realització de còpies de seguretat de les dades tractats per mitjà d'estes aplicacions, i realitzant efectivament la realització de les dites còpies.

La responsabilitat de les mesures d'identificació d'usuaris també és compartida. D'una banda, l'aplicació ha d'implementar un mecanisme d'autenticació que permeta la identificació inequívoca i personalitzada dels usuaris, recomanant-se que este mecanisme consistisca en codis d'usuari i contrasenyes, evitant la identificació per mitjà de dades biomètriques (reconeixement facial o empremta dactilar).

Si s'utilitzen contrasenyes, l'entitat ha d'incloure en la seua política el canvi periòdic de les mateixes, per la qual cosa les aplicacions que es vagen a utilitzar han d'incloure mecanismes per a permetre els dits canvis. Als usuaris els correspon l'obligació d'utilitzar de contrasenyes robustes i custodiar-les sense desvelar-les a tercers.

D) Prova de l'aplicació

Es considera convenient posar a prova l'aplicació de forma prèvia a la seua definitiva utilització en l'entitat, realitzant la prova sense introduir dades personals reals en la seua utilització. En esta fase de prova s'hauria de comprovar la correcció de les informacions que van ser facilitades pel responsable de l'aplicació.



E) Documentació de l'avaluació

Es recomana documentar les avaluacions realitzades deixant constància dels aspectes que han sigut analitzats i dels resultats obtinguts.

APLICACIONS CONCRETES

Skype

Skype és un software que permet que tot el món es comuniqui. Milions de persones i empreses ja usen Skype per a fer crides i videollamadas gratis individuals i grupals, enviar missatges instantanis i compartir arxius amb altres persones que usen Skype. Pots usar Skype en el que millor s'adapte a les teues necessitats: en el teu telèfon mòbil, PC o pastilla.

A continuació, traslladem les qüestions que poden resultar més rellevants en matèria de protecció de dades i seguretat de la informació en l'ús d'esta plataforma:

- [¿Usa Skype xifrat?](#)
- [¿Quant temps romanen els arxius i dades disponibles en Skype?](#)
- [¿Quines mesures de seguretat s'han pres per a protegir als xiquets en Skype?](#)
- [Declaració de privacitat de Microsoft](#)

Hangouts de Google

Amb Hangouts pots comunicar-te de moltes formes -xat, videollamadas, telèfon- i totes gratis. La nova aplicació Hangouts de Chrome et permet usar tot el que t'agrada d'Hangouts en un ordinador amb Chrome OS o Windows i seguir connectat amb els teus amics usen el dispositiu que usen.

A continuació, traslladem les qüestions que poden resultar més rellevants en matèria de protecció de dades i seguretat de la informació en l'ús d'esta plataforma:

- [Termes y privacitat de Google](#)

Webex

Webex és una solució que ofereix un conjunt de ferramentes de programari eficaç que brinden una experiència de col·laboració segura, fiable i per demanda en la web. Forma part de la línia de solucions de vídeo de la marca Cisco. Ofereix la possibilitat de convertir un missatge instantani en una reunió instantània utilitzant l'àudio i el vídeo integrats.

A continuació, traslladem les qüestions que poden resultar més rellevants en matèria de protecció de dades i seguretat de la informació en l'ús d'esta plataforma:

- [¿Són segurs els productes de Webex?](#)
- [Declaració de privacitat](#)



Microsoft Teams

Microsoft Teams és una plataforma creada per Microsoft que sustenta el treball en equip en les organitzacions; este tipus de programari, que posa a disposició sales de xat, fonts de notícies i grups per al treball, forma part del paquet 365 de Microsoft Office.

A continuació, traslladem les qüestions que poden resultar més rellevants en matèria de protecció de dades i seguretat de la informació en l'ús d'esta plataforma:

- [Recomanacions sobre TI](#)
- [Privacitat en Microsoft](#)

Zoom

Zoom proporciona un servei de conferència remota que combina videoconferència, reunions en línia, xat i col·laboració mòbil. Es pot accedir tant des del Smartphone com des d'un PC. **No obstant això, té alguns problemes amb la privacitat: permet "rastrear" l'atenció dels usuaris i recopila una gran quantitat de dades innecessàries** (nom, adreça de correu electrònic, direcció física, número de telèfon, dispositiu utilitzat, direcció IP..) recopila a més qualsevol informació que "se carregue, es proporcione o creu mentre s'usa el servei". A continuació, traslladem les qüestions que poden resultar més rellevants en matèria de protecció de dades i seguretat de la informació en l'ús d'esta plataforma:

[Polítiques legals y de privacitat](#)

Orientacions per al correu electrònic

Si es planteja un escenari en què els usuaris puguin accedir al sistema de correu electrònic corporatiu des d'equips informàtics no gestionats per l'entitat a través d'internet, es recomana reforçar la inspecció dels e-mails abans de ser entregats als usuaris. En cas contrari, les probabilitats de ser víctima d'un atac s'incrementen considerablement, atès que els ordinadors particulars, en remot, no garantixen una seguretat adequada. Si s'inspeccionen els correus electrònics, com a mínim, l'entitat que té controlat el perímetre de seguretat, sí que detectaria qualsevol intent d'atac.

A més, és important controlar els motors d'antivirus i inspeccionar les bústies de correu electrònic cap arrere en el temps de les persones que tinguen tant accés remot com accés al correu electrònic corporatiu. No s'hauria d'utilitzar dades sensibles de l'organització o informació que legalment haja de ser protegida en equips que no pertanguen a l'organització.

"Si es planteja un escenari en què els usuaris puguin accedir al sistema de correu electrònic corporatiu des d'equips informàtics no gestionats per l'entitat a través d'internet, es recomana reforçar la inspecció dels e-mails abans de ser entregats als usuaris. en cas contrari, les probabilitats de ser víctima d'un atac s'incrementen considerablement, atès que els ordinadors particulars, en remot, no garantixen una seguretat adequada"



MATERIAL COMPLEMENTARI

- Destacar novament les Recomanacions de l'AEPD per a protegir les dades personals en situacions de mobilitat i teletreball. [Consulta este enllaç](#). Destaquem;

1. "Respectar la política de protecció de la informació en situacions de mobilitat definida pel responsable"
2. "Protegir el dispositiu utilitzat en mobilitat i l'accés al mateix"
3. "Garantir la protecció de la informació que s'està manejant"
4. "Guardar la informació en els espais de xarxa habilitats"
5. "Si hi ha sospita que la informació ha pogut veure's compromesa comunicar amb caràcter immediat la breixa de seguretat"

- Recomanacions de Seguretat per a situacions de teletreball i reforç en vigilància del Centre Criptològic Nacional, CCN - CERT. [Consulta este enllaç](#).

- Avantprojecte de Llei de Treball a Distància. [Consulta este enllaç](#)

NOTICIES

- **El Tribunal de Justícia de la Unió Europea (TJUE) ha invalidat el sistema d'intercanvi de dades del cridat «Privacy Shield»** («Escudo de privacidad», en espanyol) entre la Unió Europea (UE) i els EE.UU a l'entendre que hi ha una «excesiva vigilància» per les autoritats nord-americanes. Des de les Agència Espanyola de Protecció de Dades s'analitza com afecta nostra Privacitat esta i altres mesures en els temps de pandèmia. [Consulta este enllaç](#) amb les indicacions
- **Pot tindre accés il·limitat la Policia a les teues dades personals?** El Constitucional alemany restringix l'accés de la policia a les dades privats dels ciutadans. [Consulta este enllaç](#) amb les implicacions.
- **Sanció de 40.000 EUR (24.000 al beneficiar-se de les 2 reduccions de la Llei 39/2015) a Ibèria, imposada per l'Agència Espanyola de protecció de Dades per no facilitar el dret d'accés** a unes gravacions. Anteriorment l'AEPD havia resolt el procediment concedint l'accés. [Consulta este enllaç](#) amb la sanció.
- **La tecnologia 5G arriba per a quedar-se** i encara que oferix importants millores als usuaris també pot implicar certs riscos per a la privacitat. L'Agència ha publicat una anàlisi que inclou recomanacions relacionades amb la Protecció de Dades. [Consulta este enllaç](#)
- **Pot ser el Reconeixement facial la nostra entrada en concerts i altres esdeveniments?** Futur pla que preocupa per la seua falta de privacitat. [Consulta este enllaç](#). Per la seua banda l'Agència Espanyola de Protecció de Dades realitza una guia amb recomanacions respecte d'això, [Consulta este enllaç](#).