# POLÍTICA D’ÚS DELS DISPOSITIUS MÒBILS PERSONALS PER ÚS PROFESSIONAL A [..........]

[..........] va acordar que els professionals que presten els seus serveis a l’entitat puguin configurar el seu correu electrònic corporatiu en el seu dispositiu mòbil personal.

El fet de poder treballar amb dispositius mòbils personals per ús professional ens aportarà molts avantatges com l’augment de la productivitat, la satisfacció i la flexibilitat dels professionals; l’eficiència en el servei; així com la reducció de costos i estalvi en la inversió de dispositius, entre altres.

D’altra banda, també implica un seguit de riscos per la seguretat de la informació que tracta l’entitat, com per exemple, la pèrdua o robatori d’informació; el mal ús del propi dispositiu; el robatori del dispositiu; el robatori de credencials d’accés; la utilització de sistemes de connexió no segurs, etc.

En aquest sentit, s’ha considerat convenient elaborar una política de compromisos, recomanacions i bones pràctiques amb relació a l’ús dels dispositius mòbils personals a l’àmbit professionals amb l’objectiu de preservar la seguretat de la informació i complir amb la normativa de protecció de dades. Per això, és necessari que tots els professionals de [..........] que utilitzin dispositius personals a l’àmbit corporatiu subscriguin aquest document.

D’altra banda, s’informa que [..........] tractarà les dades personals que ha proporcionat per gestionar i controlar el compliment de la política d’ús de dispositius mòbils personal a l’àmbit professional; finalitat que es basa en l’execució de contracte. Aquesta informació es comunicarà als organismes públics competents i, si s’escau, a les autoritats judicials; i es conservarà durant el termini que preveu la normativa per fer front a l’exercici i defensa de reclamacions. Pot exercir els seus drets d’accés, rectificació, supressió i portabilitat de les seves dades, de limitació i oposició al seu tractament, així com a no ser objecte de decisions basades únicament en el tractament automatitzat de les seves dades, i a revocar el seu consentiment en qualsevol moment quan procedeixin i sense que això afecti a la licitud del tractament prèvia a la revocació, davant [..........]al c/ [..........] o bé a [.....@.....]. Té dret a presentar una reclamació davant l’autoritat de control competent i per obtenir més informació sobre el seu dret a la protecció de dades pot acudir a l’Agència Espanyola de Protecció de Dades. Les dades de contacte del delegat de protecció de dades són: [.....@.....]

....................................................... amb DNI......................................., en el marc de la relació contractual que m’uneix amb [..........], em dono per assabentat i em comprometo a observar les mesures de seguretat que es detallen a continuació:

# Riscos de seguretat

## Pèrdua, robatori o destrucció de dispositius

La desaparició o destrucció d’un dispositiu mòbil no només comporta la pèrdua econòmica del seu valor, sinó també la pèrdua d’informació que té valor per l’entitat així com l’ús fraudulent d’aquesta informació en cas que arribi a tercers.

Els dispositius mòbils personals per ús professional tenen més possibilitats de patir un incident d’aquestes característiques atès que el seu ús s’estén també a l’àmbit personal i en situacions i llocs més insegurs (p.ex. zones d’oci, activitats esportives, manipulacions per infants, etc.)

* 1. Robatori de credencials

Utilitzar dispositius mòbils personals per ús corporatiu fora de les instal·lacions de l’entitat (p.ex. hotels, mitjans de transport, estacions de tren o aeroports, bars, restaurants, la pròpia casa del professional, etc.) els fa especialment sensibles al possible robatori de credencials d’accés. És suficient un simple descuit com els següents per què un usuari no autoritzat pugui accedir a la informació que conté el dispositiu:

* Abandonar el dispositiu sense bloquejar-lo
* Tenir anotada una contrasenya a la vista dels altres (en un paper, amb un *post-it*, etc.)
* Teclejar la contrasenya a la vista dels altres
* Tenir memoritzades les contrasenyes de les aplicacions que utilitzem
	1. Pèrdua d’informació

Tot i que un dispositiu estigui configurat amb mesures de seguretat adequades pel seu ús privat, això no significa que es compleixi amb les mesures de seguretat que es necessiten en l’entorn corporatiu per garantir la integritat de les dades que es gestionen.

La falta de seguretat i el mal ús del dispositiu mòbil pot comprometre la informació que conté o, inclús, perdre-la definitivament.

La pèrdua d’informació confidencial podria desembocar una fuga d’informació amb posterior difusió i/o publicació amb conseqüències greus com aquestes:

* Pèrdua d’usuaris
* Deteriorament de la imatge i la reputació de [..........]
* Pèrdua de posicionament vers altres associacions i/o entitats que presten serveis similars
* Sancions econòmiques per infracció de la normativa de protecció de dades (p.ex. fruit de la incoació d’un procediment sancionador per part de l’Autoritat de Control competent)
	1. Connexió a xarxes insegures

En determinades ocasions el professional ha de connectar el dispositiu mòbil a una xarxa fora de la protecció que brinda la xarxa privada de [..........]. Sigui per estalvi en la tarifa de dades, per no disposar de cobertura o de 3G/4G, és habitual que s’utilitzin xarxes públiques obertes o poc segures per l’intercanvi de correus electrònics corporatius o accedir a aplicacions.

Aquesta tipologia de xarxa la podem trobar com serveis de cortesia a bars, restaurants, hotels, aeroports, etc. S’ha de desconfiar d’aquestes xarxes ja que no sabem qui pot estar darrere d’elles ni qui les administra.

Abans d’utilitzar-les ens hem d’informar de quin és el nom de la xarxa (SSID) i si està degudament protegida per tal que ens hi podem connectar amb un mínim de confiança.

Cal prestar atenció perquè els ciberdelinqüents creen xarxes wifi en zones públiques amb noms similars als del lloc on es troben amb l’objectiu de capturar connexions i recopilar informació.

* 1. Geoposicionament

Un dels riscos d’estar connectat permanentment a la xarxa és l’ús del geoposicionament, una informació que s’obté mitjançant el GPS, les xarxes wifi i l’antena de telefonia del proveïdor de servei del professional. Aquesta informació a més, també pot ser utilitzada per altres serveis i aplicacions del dispositiu mòbil personal.

Es recomana al professional que configuri correctament aquesta informació del seu dispositiu mòbil personal per evitar monitoritzacions per part dels serveis i empreses externes que tenen accés a la seva geoposició.

* 1. Usuaris

L’usuari és el punt més important de la cadena de seguretat d’una organització. Doncs, no és suficient implementar mesures de seguretat adequades sinó que cal que l’usuari estigui conscienciat, compromès i format en matèria de ciberseguretat per:

* Ajudar a complir les normes i polítiques establertes en l’ús de dispositius
* Gestionar els possibles incidents i alertes de seguretat dels dispositius
* Avisar de qualsevol incidència sobre la informació i els dispositius, sigui intencional o no

Tan és així que la pèrdua de control de la gestió de dispositius mòbils personals a l’àmbit professional es deu principalment a configuracions i instal·lacions que realitzen els usuaris i que poden afectar a la seguretat de la informació que contenen, com per exemple:

* Instal·lar aplicacions insegures que poden contenir malware
* Canvis de paràmetres de configuració que donin més permisos dels necessaris a les aplicacions
* Manipular els dispositius per eliminar les limitacions de fàbrica dels smartphones (p.ex. *rootejar* un Android o realitzar *jailbreak* a iOS)

# Mesures de seguretat

Per implementar mesures de seguretat podem incorporar eines específiques que gestionen dispositius mòbils i l’ús de la informació corporativa que realitzin. D’aquesta manera podrem controlar el grau d’implementació de les mesures de seguretat i gestionar:

* Els dispositius autoritzats per accedir a les aplicacions i recursos
* Les aplicacions instal·lades
* Les configuracions de seguretat dels dispositius, wifi i VPN
* Les manipulacions indegudes del terminal
* El bloqueig remot de dispositius extraviats
* La destrucció/formateig remot de dades de dispositius extraviats o robats
* El xifrat de dades o del dispositiu
* La detecció de malware
* La fortalesa i renovació de contrasenyes

## Protecció de la informació

### Aplicacions instal·lades

Quan s’instal·lin aplicacions, s’ha de tenir en compte el següent:

* Descarregar i instal·lar únicament les que estan permeses per [..........]
* Llegir les condicions d’ús i instal·lació per controlar els permisos d’accés sobre el dispositiu
* Descarregar-les dels Markets oficials (Play Store, App Store) per evitar la instal·lació de malware

### Emmagatzematge al núvol

Per garantir la seguretat de la informació, s’han d’utilitzar únicament els serveis al núvol autoritzats per [..........], mitjançant una comunicació xifrada. Abans d’utilitzar un d’aquests serveis s’ha de tenir en compte:

* Les condicions d’ús relatives a les garanties de disponibilitat i confidencialitat de la informació en cas de manteniment del servei o incidència en matèria de seguretat
* Les possibles restriccions del proveïdor respecte al tipus de dades que podem emmagatzemar
* A on acudir en cas de tall del servei, mesures de protecció de la informació i els temps d’indisponiblitat permesos per contracte
* El tipus i freqüència amb la que el proveïdor realitza les còpies de seguretat dels seus servidors
* Implementar mecanismes addicionals de seguretat com el xifrat de la informació i l’accés mitjançant autenticació de l’usuari

### Còpies de seguretat

* Les còpies de seguretat permeten recuperar ràpidament la informació si el dispositiu es torna inaccessible per pèrdua o robatori, esborrat accidental, material del terminal defectuós. En aquest sentit hem de tenir present que:
* Les còpies realitzades s’han d’emmagatzemar fora del dispositiu. Dos alternatives factibles són: els servidors de l’entorn corporatiu i el núvol
* Les còpies de seguretat s’han de realitzar automàticament o manualment cada cert temps.
* Comprovar que el sistema de còpies de seguretat funciona correctament

### Xifrat de dispositius

Els sistemes de xifrat del dispositiu permeten que no es comprometi la confidencialitat de la informació emmagatzemada i que no hi accedeixin tercers no autoritzats.

## Configuració dels dispositius

* + 1. Mesures tècniques de configuració
* Habilitar sistemes d’autenticació robustos. Ens poden ser d’ajuda les aplicacions gestores de contrasenyes per assegurar la diversitat i dificultat de les mateixes
* Instal·lar i configurar un antivirus
* Configurar les actualitzacions del software
* Configurar el xifrat de dades i comunicacions
* Desactivar el permís de record de contrasenya, obligant a introduir-la cada vegada que es faci ús de les aplicacions
	+ 1. Localització remota

Les eines de localització remota dels dispositius mòbils proporcionen funcionalitats interessats en cas de pèrdua o robatori:

* Localització de terminals mitjançant GPS, wifi o l ainformació d’antena de telefonia del proveïdor del servei de connexió
* Bloqueig remot del terminal per evitar l’ús no autoritzat
* Esborrat remot de dades
* Seguiment de l’activitat del dispositiu per vigilar les aplicacions que s’executen

Tant iOS (Find my iPhone) com Android (Device Manager) entre altres, disposen de funcionalitats de seguiment que es poden configurar.

En cas de robatori, les dades obtingudes mitjançant aquestes aplicacions s’han de posar a disposició de les autoritats competents.

* + 1. Geolocalització

Es recomana deshabilitar aquesta funcionalitat sempre que el seu ús no sigui estrictament necessari.

Quan s’instal·lin aplicacions s’ha de tenir precaució amb aquelles que sol·liciten accés a la funció de geoposicionament del dispositiu. S’ha d’habilitar aquesta funció només quan sigui necessari.

* 1. Protecció de connexions a xarxes externes
		1. Xarxes wifi
* Desconfiar de les xarxes wifi públiques o gratuïtes
* Utilitzar canals xifrats segures de comunicació VPIN o algun altre tipus de xifrat punt a punt com el de les pàgines web amb protocol SSL i certificats
* Desconnectar la wifi dels dispositius quan no s’estigui utilitzant
* Desactivar la connexió automàtica a xarxes. D’aquesta forma quan el dispositiu detecti noves xarxes disponibles, preguntaràs si l’usuari es vol connectar a alguna d’elles
* Preferentment, fer ús de xarxes 3G o 4G abans que de xarxes wifi insegures
	+ 1. Xarxes privades virtuals (VPN)
* Una VPN crea un túnel a través d’internet, o qualsevol altra xarxa no segura, de forma que es pot accedir des de qualsevol lloc als serveis i documents interns de l’organització.
* Permet connectar-se de forma segura a través de xarxes com les wifis de cortesia ja que desconeixem el grau de seguretat que ofereixen. D’aquesta manera es garanteix la confidencialitat i integritat de la informació que es transmet

# Normes particulars per l’ús del compte de correu electrònic corporatiu proporcionat per [..........]

1. Els comptes de correu electrònic són corporatius propietat de [..........] i funcionen com una eina de treball propietat de l’entitat.
2. Queda terminantment prohibit fer ús del compte de correu electrònic que [..........] ha proporcional al professional per finalitats particulars o personals.
3. Queda prohibit enviar correus electrònics massius (*spam*) utilitzant la direcció de correu electrònic corporativa.
4. En el supòsit que l’usuari estigui autoritzat per enviar correus electrònics a més d’un destinatari, s’utilitzarà el camp de còpia oculta (CCO).
5. Queda prohibit l’ús del correu electrònic corporatiu vulnerant el dret de tercers, propis de [..........], o bé per la realització d’actes que poguessin ser considerats il·lícits.
6. En aquells correus electrònics en els que s’hagi d’adjuntar arxius o documents que continguin dades de caràcter personal, s’implementaran les mesures de seguretat adequades per evitar que l’accés no autoritzat a la informació.
7. Tots els correus electrònics que s’enviïn tindran el format establert per [..........]. Com a mínim, hauran de contenir la informació següent:
	1. Nom del professional a la definició del compte de correu en el camp “nom per mostrar”
	2. La firma del correu amb identificació clara del remitent, departament, entitat i correu electrònic
	3. Informació sobre el tractament de les dades personals de la comunicació electrònica en compliment del deure d’informació prèvia als afectats d’acord amb la normativa de protecció de dades.

# Restriccions, advertències i previsions

1. Només els dispositius mòbils personals autoritzats podran tenir accés a la informació de [..........]. A sensu contrario, es prohibeix utilitzar equips i dispositius aliens no autoritzats per [..........] per connectar-se als actius de l’entitat; especialment, si es tracta d’equips públics compartits com poden ser els d’un locutori, hotels, centres comercials, etc.
2. Als efectes del previst en l’apartat anterior, es crearà una base de dades amb els dispositius mòbils personals dels professionals autoritzats que inclourà:
	1. Nom i cognoms del professional autoritzat
	2. Número de telèfon
	3. Marca i model del dispositiu
	4. Versió actual del sistema operatiu
	5. Privilegis de seguretat
3. Aquesta política d’ús es podrà modificar i actualitzar a les noves mesures de seguretat que apareguin o resultin òptimes, així com per actualitzar la base de dades de dispositius mòbils personals i usuaris autoritzats.
4. En cas d’incidència en matèria de seguretat de la informació que comprometi o pugui comprometre informació de caràcter personal, l’usuari haurà de comunicar-ho als responsables de l’entitat i/o al Delegat de Protecció de Dades de [..........] a la major brevetat possible i dins el termini màxim de 24 hores des que en té coneixement.
5. Aquesta política d’ús de dispositius mòbils personals de [..........] forma part del conjunt de mesures de responsabilitat proactiva que ha implementat als efectes de complir la normativa de protecció de dades. En aquest sentit, s’adverteix al sotasignat/da que aquest document és complementari i no substitueix els compromisos i obligacions adquirits en virtut del pacte de confidencialitat que va signar amb [..........].
6. En cas d’incompliment d’algunes o totes les previsions d’aquesta política d’ús de dispositius mòbils personals en el sí de l’entitat, s’adverteix al sotasignat/da que [..........] es reserva el dret d’exercir contra ell/a les accions legals que per dret li corresponguin als efectes de sol·licitar que se l’indemnitzi pels danys i perjudicis que s’hagin ocasionat inclòs el lucre cessant.

Lloc i data:

Signatura: