POLÍTICA DE COMPLIMENT NORMATIU

POLÍTIQUES DE LES TECNOLOGIES DE LA INFORMACIÓ I LA COMUNICACIÓ (TIC)

Pallars 191
08005 Barcelona
info@socialistes.cat
Tel. 93 495 54 08

Partit dels Socialistes de Catalunya (PSC-PSOE)
socialistes.cat

Elaboració	Revisió:	Aprovació:
Nom. Alicia Herrero **Càrrec. Dep. Disseny i Edicions PSC** **Signatura.** **Data: 2019.12.18**	**Nom.** **Càrrec.** **Signatura.** **data:**	**Nom.** **Càrrec.** **Signatura.** **data:**

Versió	Data	Afecta	Breu descripció de la modificació
1ª	3-12- 18	Creació	
2ª	4-12-19	Correcció estil i ortogràfica	
3ª	18-12-19	Maquetació	

I. INTRODUCCIÓ

El present protocol recull la normativa i procediments del PARTIT DELS SOCIALISTES DE CATALUNYA (PSC-PSOE), (a partir d'ara "PSC"), en relació amb les eines posades a disposició dels treballadors per al desenvolupament de les seves activitats laborals, amb l'objectiu de crear al partit una cultura ètica i de compliment d'actuació d'acord amb la legalitat i evitar així qualsevol tipus de conductes delictives en relació amb aquests mitjans.

La utilització creixent de les noves tecnologies per part de les persones jurídiques ha creat la necessitat, en certes circumstàncies, de control d'aquestes eines per part dels òrgans de govern de les organitzacions. Sense que això suposi una vulneració de la intimitat del treballador, la qual cosa seria constitutiu de delicte contra la intimitat.

Tot i així, aquest dret a la intimitat del treballador, s'ha de conciliar amb els drets i interessos legítims de l partit, com el dret a vetllar per l'eficàcia del partit i protegir-lo del perjudici que poguessin ocasionar les accions de treballador.

És interessant fer una breu referència a la normativa i jurisprudència existent en aquesta matèria:

El Conveni Europeu per a la Protecció dels Drets Humans estableix que tothom té dret al respecte de la vida privada i familiar i prohibeix la ingerència que no estigui prevista en la llei i que no es justifiqui per raons de seguretat, benestar econòmic, defensa de l'ordre, prevenció de les infraccions penals, protecció de la salut, de la moral o dels drets i llibertats dels altres.

Així mateix, la Constitució espanyola recull com a dret fonamental el dret a la intimitat personal i familiar i a la pròpia imatge, així com el secret de les comunicacions.

Per la seva banda, l'Estatut dels Treballadors en el seu art. 20 disposa que l òrgan de govern de l'entitat podrà adoptar les mesures de vigilància i control que consideri més oportunes per verificar el compliment per part del treballador de les seves obligacions i deures laborals, guardant en la seva adopció i aplicació la consideració deguda a la seva dignitat humana i tenint en compte la capacitat real dels treballadors amb discapacitat, si escau.

Els Tribunals han interpretat aquesta qüestió i, com a exemple, la sentència de Tribunal Suprem de 26 de setembre de 2007 (Sala del Social) estableix el següent:

".... **les mesures de control sobre els mitjans informàtics posats a disposició dels treballadors es troben, en principi, dins de l'àmbit normal d'aquests poders: l'ordinador és un instrument de producció del qual és titular l'empresari "com a propietari o per un altre títol" i aquest té, per tant, facultats de control de la utilització, que hi inclouen lògicament l'examen.** D'altra banda, amb l'ordinador s'executa la prestació de treball i, en conseqüència, el partit hi pot verificar el seu correcte compliment, cosa que no succeeix en els supòsits de l'article 18, ja que fins i tot respecte a l'armariet, que és un bé moble del partit, hi ha una cessió d'ús a favor del treballador que delimita una utilització per a ell que, encara que vinculada causalment al contracte de treball, queda al marge de la seva execució i dels poders empresarials de l'article 20 de l'Estatut dels Treballadors ja que es tracta de l'esfera personal del treballador.

... Es tracta de mitjans que són propietat de l'entitat i que facilita al treballador per utilitzar-los en el compliment de la prestació laboral, de manera que aquesta utilització queda dins de l'àmbit del poder de vigilància de l'entitat, que, com precisa l' article 20.3 de l'Estatut dels Treballadors, implica que aquest "podrà adoptar les mesures que consideri més oportunes de vigilància i control per verificar el compliment per part del treballador de les seves obligacions i deures laborals", tot i que aquest control ha de respectar "la consideració deguda" a la "dignitat" del treballador".

Així mateix, l'esmentada sentència va establir que hi ha un hàbit social generalitzat de tolerància amb certs usos personals moderats dels mitjans informàtics i de comunicació facilitades pel partit als treballadors. Aquesta tolerància crea una expectativa de confidencialitat que s'ha de tenir compte. Per això, disposa a continuació que **les entitats han de fixar prèviament les regles d'ús dels instruments de treball** (p. ex. establint prohibicions absolutes o parcials, o permetent l'ús personal per part dels empleats) **i n'han d'informar els treballadors** i els seus representants legals, si en disposen- de quines són aquestes regles, dels controls i mesures aplicables per part de l'entitat. D'aquesta manera desapareix l'expectativa d'intimitat dels treballadors sobre aquests mitjans i el seu control no hauria de generar un possible delicte contra la intimitat.

Encara aquesta doctrina s'ha flexibilitzat en virtut de sentències posteriors del Tribunal Suprem i del Tribunal Constitucional, és recomanable que les entitats disposin d'un protocol d'actuació en matèria d'ús de TIC.

1.1. Objectiu i abast

Per mitjà del present protocol el PARTIT DELS SOCIALISTES DE CATALUNYA (PSC-PSOE) (a partir d'ara "PSC") pretén establir un sistema d'ús i control del conjunt de les tecnologies de la informació que s'utilitzen per part dels membres del partit.

Així mateix, es pretén regular el control, per evitar la comissió de delictes contra la intimitat en l'àmbit del PSC, i que no se'n derivi una intromissió en la intimitat del treballador i el seu dret al secret de les comunicacions, és a dir, respectant la seva esfera d' privacitat.

1.2. Principis generals sobre la vigilància i control del correu electrònic i la utilització d'Internet

Per tal que l'activitat de control per part de l'ocupador sigui legal i estigui justificada, s'han de respectar els principis de protecció de dades personals.

Cal que les limitacions imposades siguin necessàries per assolir la seva finalitat legítima, però també que siguin limitacions proporcionades per aconseguir aquesta finalitat i respectuoses amb el dret a la intimitat.

Els principis que han de respectar són els següents:

a. **Necessitat**: l'ocupador, abans de procedir a realitzar aquesta activitat de control, ha de comprovar que el mecanisme de vigilància que ha de dur a terme és necessari per al cas concret. Sempre serà més apropiada o, si és possible, la utilització de mitjans més comuns i de menor ingerència en la privacitat del treballador; només es recorrerà a la

vigilància del correu electrònic o ús de Internet en circumstàncies excepcionals.

b. **Finalitat**: prèviament cal establir quin és l'objectiu o finalitat legítima de l'activitat de control i recollida de dades. La informació i dades obtingudes s'utilitzaran únicament i exclusivament per a aquesta finalitat concreta.

   Ex. El tractament de les dades pot realitzar-se a efectes de seguretat de sistema, però aquestes dades no es poden utilitzar per supervisar el comportament del treballador.

c. **Transparència**: l'ocupador ha d'indicar de manera clara i oberta les seves activitats. Això implica que l'ocupador ha de:
   - Informar els seus treballadors sobre la política existent a l'associació relativa a la vigilància del correu electrònic i de la utilització d'Internet.
   - Comunicar als seus treballadors en quina mesura poden utilitzar els sistemes de comunicació del partit amb finalitats privades o personals.
   - Determinar en quines circumstàncies el PSC pot adoptar mesures de vigilància.
   - Informar els treballadors de les mesures de vigilància adoptades.
   - Informar cada treballador de qualsevol abús de les comunicacions electròniques detectat, llevat que les circumstàncies justifiquin la continuació de la vigilància.

d. **Legitimitat**: l'operació de vigilància i control de les dades únicament pot realitzar-se si la finalitat és legítima.

e. **Proporcionalitat**: les dades que s'utilitzin han de ser adequades, pertinents i no excessives en relació amb les finalitats per a la qual s'han recaptat, tenint en compte el tipus i grau de risc a què s'enfronta el partit. Queda per tant exclòs, el control general dels correus electrònics i de la utilització d'Internet amb el personal del partit, llevat que sigui estrictament necessari per a la seguretat de sistema. Si l'objectiu perseguit es pot aconseguir per un mitjà que impliqui una intromissió menor en la vida privada dels treballadors, s'ha d'aplicar preferentment aquesta opció.

f. **Exactitud i conservació de les dades** : les dades recopilades han de ser precises i no es podran emmagatzemar més temps de l'estrictament necessari. Normalment s'estableix un període de conservació dels missatges electrònics en el servidor central del partit de 3 mesos.

g. **Seguretat**: és necessari que l'ocupador adopti les mesures tècniques i organitzatives adequades per a protegir de qualsevol intromissió exterior totes les dades personals que es trobin en el seu poder. La persona que durant les operacions de control accedeixi a les dades personals de treballadors ha d'estar sotmesa a una obligació estricta de secret professional respecte a la informació confidencial a la qual hi té accés.

1.3. Control del correu electrònic

Perquè l'ocupador pugui procedir al control del correu electrònic corporatiu dels seus treballadors, aquests han d'haver atorgat el seu **consentiment.** No obstant això, aquest consentiment no pot ser utilitzat per l'ocupador com a mitjà general per legitimar aquests controls. Els treballadors tenen el dret fonamental, reconegut a la Constitució, al secret de la correspondència.

Igualment, cal que el PSC faciliti una informació mínima als seus treballadors:

- Determinar si el treballador té permesa la utilització de comptes de correu web al lloc de treball.
- Regles sobre l'accés al contingut del correu electrònic corporatiu i les finalitats específiques d'aquest accés.
- Indicar el període de conservació de les còpies de seguretat dels missatges.
- Precisar quan s'esborren definitivament els correus electrònics del servidor corporatiu.
- Qüestions de seguretat.
- Participació dels representants dels treballadors en la formulació de la política.

1.4. Control d'accés a Internet

El PSC és qui ha de decidir si autoritza la utilització privada d' Internet i en quina mesura.

Pel que fa al control de la utilització d'Internet, es recomana la implementació de mitjans tècnics per a prevenir la utilització abusiva d'Internet, per ex. limitant accessos o utilitzant avisos o advertències automàtiques.

En tot cas, i quan es duguin a terme activitats de control sobre els accessos a Internet dels treballadors, la mesura de control ha de ser proporcional al risc al que està sotmès el partit En moltes ocasions, només cal dur a terme comprovacions generals, per exemple, l'elaboració d'un llistat dels

llocs més visitats per comprovar si s'està duent a terme una utilització abusiva d'Internet, sense analitzar el contingut dels llocs visitats.

Si a través de comprovacions generals es detecta la possible utilització abusiva d'Internet, l'empresari podria considerar la possibilitat de realitzar altres controls.

En tot cas, caldrà comunicar al treballador els resultats obtinguts i oferir-li la possibilitat de defensar una correcta utilització d'Internet.

La **informació mínima que haurien de rebre els treballadors en relació a la utilització d'Internet** és la següent:

- En quines condicions s'autoritza la utilització de Internet amb finalitats privades.
- Restriccions existents: elements que no poden ser visualitzats o copiats.
- Informar dels sistemes instal·lats.
- Precisar el control que pot realitzar o realitzarà el partit.
- Ús que es durà a terme amb les dades recollides.

II. NORMES DE L'ENTITAT

La política d'ús de les eines TIC (Tecnologies de la Informació i Comunicació) del PSC està encaminada a garantir la seguretat en la utilització dels sistemes d'informació i de les comunicacions, establir els sistemes de control i les conseqüències que l'incompliment de la mateixa té per als empleats.

Les normes contingudes en el present protocol són d'obligat compliment per part de tot el personal del PSC i la seva vulneració pot comportar accions disciplinàries.

El PSC implementarà les mesures necessàries per dur a terme un adequat control sobre el compliment i respecte de la política d'ús de les eines TIC.

El PSC és una entitat conscienciada amb la seguretat dels seus sistemes d'informació i vetlla pel manteniment de la seva seguretat. Així mateix, en compliment de la legalitat:

a. Tots els equips, infraestructures i aplicacions disposats al servei amb el personal contractat són propietat del PSC i només es permet la seva utilització per al desenvolupament de les tasques establertes en l'àmbit laboral.

b. Totes les dades processades pels elements anteriorment esmentats i els resultats que se'n derivin són propietat del PSC, en conformitat amb la legislació sobre propietat intel·lectual.

c. El partit no admet la utilització particular de les TIC i eines posades a disposició dels usuaris.

d. L'ús de les TIC serà controlat tant per motius de seguretat com per motius de control de l'activitat laboral.

e. El sistema de control es basarà en un sistema proporcional basat en les següents premisses:

    – Davant eines que permetin sistemes de control menys invasius, es procurarà prèviament el control d'aquests elements i, posteriorment, el control d'aspectes més concrets que continguin dades.

- En tot cas, es poden establir sistemes de control basats en mostres aleatòries, però que no suposin d'antuvi un control total de l'activitat.

f. Es podran adoptar les mesures legals oportunes davant de l'incompliment d'aquestes polítiques i, en general, davant de l'incompliment de la legalitat vigent.

Aquesta política es basa en les següents premisses:

- Respecte a les normes vigents en matèria de protecció de dades.
- Desenvolupament de procediments i adopció de mesures per al compliment de les obligacions que afecten dades personals.
- Disseny d'un pla de millora contínua dels procediments adoptats.

2.1. Correu electrònic

Es considera correu electrònic corporatiu tant l'intern, entre terminals de la xarxa corporativa, com l'extern, dirigit o provinent d'altres xarxes públiques o privades i, especialment, Internet.

En la utilització del correu electrònic corporatiu, el PSC adopta un model d'ús no abusiu o desmesurat.

Aquest servei, en tot cas, no ha de ser utilitzat per a realitzar les següents activitats:

- Enviar missatges amb continguts o fitxers adjunts ofensius o inadequats que puguin considerar-se, per a qui els rep, un atemptat contra la seva intimitat personal, honor o dignitat, abstenint-se d'efectuar refe-

rències pejoratives de caràcter personal en relació amb la ideologia, religió, creences, afiliació política o sindical, o realitzar comentaris basats en el gènere, edat, raça, preferències sexuals, discapacitats físiques o psíquiques, o en l'aparença de les persones.

- Enviar missatges i/o documents corporatius a comptes privats del treballador per a ús no vinculat al seu treball, o a comptes externes dels seus familiars o amics.
- Enviar o reenviar missatges de correu en cadena o de tipus piramidal.

Normes

S'estableixen les següents normes:

1) El correu electrònic corporatiu es pot assignar personalment i de forma específica, sense tenir en compte àrees o llocs de treball assignats i també com una eina de treball no exclusiva, col·lectiva i de lliure accés, assignada a àrees o llocs de treball i no a persones.

2) Queda prohibit el seu ús amb finalitats no relacionades amb les funcions laborals encomanades. El correu electrònic que el PSC posa a disposició dels seus empleats és únicament i exclusivament per a finalitats laborals.

3) L'ús del nom o cognoms del treballador juntament al domini del partit a la direcció de correu no significa l'assignació pel partit d'un correu d'ús privat no corporatiu, és així per motius organitzatius interns.

4) Es podrà realitzar còpia de seguretat dels correus electrònics i accedir al contingut dels mateixos davant de problemes tècnics o de seguretat o quan hi hagi sospites que no es compleixen aquestes normes.

5) Com a norma general, no es permeten l'ús de comptes de correu diferents als proporcionades pel partit.

6) El correu electrònic no s'ha d'utilitzar com a eina de difusió d'informació massiva, excepte aquelles expressament habilitades per a la comunicació amb una part o la totalitat dels afiliats i afiliades. Es prohibeix l'enviament de correus massius (*spam*) emprant l'adreça de correu electrònic corporativa.

7) Queda prohibit participar en "cartes en cadena".

8) No està permès manipular les capçaleres dels correus electrònics amb la finalitat d'ocultar o falsejar la identitat de l'emissor del missatge.

9) El correu electrònic és una de les fonts més importants de difusió de virus, per la qual cosa es recomana no obrir missatges sospitosos.

Controls

El partit podrà controlar l'ús del correu electrònic mitjançant un sistema de dos nivells:

- Un primer nivell de control de trànsit i d'arxius adjunts .

- Un segon nivell de control de continguts.

El partit podrà utilitzar també sistemes de control de correus basats en paraules clau o altres sistemes que estimi oportuns, sempre que estigui justificat.

2.2. Accés a internet

Els mitjans tècnics que es posen a disposició dels empleats del PSC són propietat de l'entitat, que els facilita perquè siguin utilitzats en el compliment de la prestació laboral.

No obstant això, l'accés a xarxes públiques com Internet està obert per als usuaris de l'entitat, però es condiciona a un ús del sistema no abusiu o desmesurat.

En aquest sentit, es pot considerar una utilització abusiva de les eines TIC si causa una disminució en el rendiment laboral de l'empleat o si pertorba o altera el sistema informàtic del PSC.

Normes d'ús

L'accés a Internet es configura com una eina a disposició dels empleats per al compliment de les seves tasques.

- Queda prohibit el seu ús per a finalitats no relacionades amb les funcions laborals encomanades: debats en temps real (Xat), xarxes socials, sistemes de missatgeria instantània tipus Messenger o WhatsApp, així com la instal·lació de programes P2P (*Peer-to-Peer*) i de qualsevol altre tipus d'accés a entorns o plataformes d'intercanvi de fitxers, excepte en els casos en què els treballadors tinguin encomanades tasques específicament relacionades amb l'ús d'aquestes eines
- En qualsevol cas, queda del tot prohibit l'accés a pàgines d'oci, entreteniment o webs de contingut sexual, xenòfob o que incitin a la violència.

Controls

El PSC podrà controlar l'ús de l'accés a Internet proporcionat mitjançant un control de les pàgines visitades, emmagatzematge i control de les *cookies*, i la seva utilització en procediments disciplinaris o en qualsevol ordre administratiu o judicial.

El partit també podrà utilitzar altres sistemes de control de la navegabilitat que estimi oportuns.

2.3. Equips

Normes d'ús

Els equips proporcionats pel partit es configuren com a eina a disposició dels empleats per al compliment de les seves tasques.

1) Queda prohibit el seu ús per a finalitats no relacionades amb les funcions laborals encomanades.
2) Queda prohibit treballar amb equips personals que no siguin proporcionats pel partit, excepte autorització expressa per escrit.
3) Només podran treballar amb equips portàtils les persones autoritzades per l'organització.
4) Quan es proporcionin equips portàtils o en general dispositius mòbils, l'empleat serà el responsable de la seva custòdia quan estiguin fora del partit.
5) Es procurarà en tot cas l'accés del treballador a servidors corporatius. Quan es treballi en mode local, l'empleat serà responsable que la informació sigui guardada degudament al servidor habilitat a l'efecte per evitar la pèrdua de la mateixa.

Controls

El partit podrà controlar l'ús dels equips, fins i tot el seu contingut, mitjançant el sistema que estimi oportú.

2.4. Dispositius d'emmagatzematge extern

Normes d'ús

1) Els usuaris no poden utilitzar dispositius d'emmagatzematge extern, excepte en els casos en què se n'autoritzi expressament per escrit i s'adoptin les degudes mesures de seguretat. No es podran connectar dispositius d'emmagatzematge extern.
2) La informació continguda en aquests dispositius, contingui o no dades de caràcter personal, es mantindrà xifrada.

Controls

El partit podrà controlar l'ús dels dispositius externs, fins i tot el seu contingut, mitjançant el sistema que estimi oportú.

2.5. Aplicacions

No es podran descarregar o utilitzar programes que no estiguin prèviament i expressament autoritzats pel PSC.

2.6. Càmeres de videovigilància

Per motius de seguretat, és possible l'ús de càmeres de videovigilància en zones comuns i no invasives; no obstant això, els seus enregistraments podrien ser utilitzats per a aspectes laborals o penals d'importància.

Hi ha càmeres de videovigilància a la zona exterior i zones d'accés a l'interior de les locals del PSC habilitades amb aquest tipus d'infraestructura de seguretat.

2.7. Altres aspectes

- No està permès fer servir identificadors i contrasenyes d'altres usuaris per accedir al sistema.
- No està permès burlar les mesures de seguretat establertes en el sistema informàtic, intentant accedir a fitxers o programes no autoritzats.
- No està permès modificar la configuració de xarxes, equips i de qualsevol dispositiu de treball.
- No està permès l'ús de la xarxa corporativa, sistemes informàtics i qualsevol mitjà posat a l'abast de l' usuari, vulnerant el dret de tercers, els propis de l'organització, o bé per a la realització d'actes que puguin ser considerats il·lícits.
- No està permès destruir, alterar, inutilitzar o malmetre per qualsevol via les dades, programes o documents electrònics del PSC o de tercers.
- No està permès introduir voluntàriament programes maliciosos (troians, *key loggers*), virus o qualsevol fitxer que causi o sigui susceptible de causar qualsevol tipus d'alteració en els sistemes informàtics del PSC o de tercers.
- No està permès accedir il·legalment sense autorització o intentar vulnerar mesures de seguretat d'ordinadors o xarxes que pertanyin a un tercer, així com qualsevol activitat prèvia a l'atac d'un sistema per reco-

llir informació sobre i aquest, com, per exemple, l'escaneig de ports.

- No està permesa cap activitat que infringeixi o faci ús indegut dels drets de propietat intel·lectual d'un tercer.

III. RÈGIM DISCIPLINARI

La infracció de les instruccions contingudes en la present política constituirà falta molt greu, i en atenció al règim sancionador intern serà susceptible de la imposició de la sanció que correspongui a la conducta dels destinataris segons el conveni d'aplicació corresponent.

IV. DENÚNCIES / MECANISMES DE REACCIÓ

Tot directiu, treballador o persona relacionada amb l'entitat que detecti l'incompliment de qualsevol norma de la present política ha de denunciar-ho al canal de denúncies habilitat per l'Entitat:

http://asesoriapenalcorporativa.es/canal-denuncias/psc-psoe/

Sempre que es detecti qualsevol pràctica contrària a aquest protocol, l'Entitat aplicarà els mecanismes de reacció previstos al Protocol de funcionament de l'Òrgan de Control i de Canal de Denúncies aprovat.

V. REVISIÓ I ACTUALITZACIÓ

La present Política s'ha de revisar i, en cas que sigui procedent, actualitzar anualment, així com sempre que s'apreciï un risc que no havia estat pre-

vist, per exemple, per l'ús de noves fórmules corruptes que no hagin estat avaluades.

A més, sempre s'ha de revisar i actualitzar quan es detecti la possible existència de conductes corruptes, així com quan s'inicïi un procediment judicial o investigador per pràctiques que puguin ser constitutives de corrupció. En aquests casos, a més haurà de valorar les noves mesures a implantar per evitar que es puguin cometre pràctiques corruptes en el si de l'Entitat.

Aquest Protocol ha estat aprovat per l'Òrgan d'Administració; en cas de revisió, s'ha d'informar de les conclusions assolides al Consell i qualsevol modificació o actualització s'ha de sotmetre a la seva aprovació expressa.