apdcat

Autoritat Catalana de Protecció de Dades

Recomanació 1/2013

de l'Autoritat Catalana de Protecció de Dades, sobre l'ús del correu electrònic en l'àmbit laboral

Generalitat de Catalunya

Introducció

L'ús de les tecnologies de la informació i la comunicació en l'activitat de les administracions públiques, i entre elles l'ús de sistemes de correu electrònic, ha comportat, sense cap mena de dubte, un gran avenç en l'eficàcia de l'activitat del sector públic. La immediatesa de la comunicació, el gran volum d'informació que pot circular per la xarxa, la possibilitat d'accedir a la informació des de fora del lloc de treball i la reducció de costos lligada a la utilització d'un sistema de correu electrònic han fet d'aquesta eina un element imprescindible en qualsevol organització administrativa. Però els innegables aspectes positius que incorpora l'ús d'aquestes tecnologies no permeten menystenir els riscos derivats de l'ús del correu electrònic per a la seguretat de la informació i la protecció de les dades de caràcter personal.

D'acord amb el que estableix l'article 8.2.e) de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades, correspon a la directora de l'Autoritat dictar les instruccions i les recomanacions necessàries per adequar els tractaments de dades personals als principis de la legislació vigent en matèria de dades de caràcter personal. Per això, resulta convenient oferir pautes i bones pràctiques en l'ús d'aquests sistemes de comunicació mitjançant una Recomanació.

Aquesta Recomanació s'adreça a les administracions públiques catalanes, i també a tots els altres ens inclosos dins l'àmbit d'actuació de l'Autoritat Catalana de Protecció de Dades. Amb independència de la seva naturalesa pública o privada, i amb independència també de la naturalesa del vincle jurídic que estableixin amb els seus treballadors, aquests ens adopten la posició jurídica de l'empresari. És per això que, en aquesta Recomanació, ens referirem a tots aquests ens sota la denominació *empresa*.

La Recomanació s'adreça, especialment, als responsables de la informació, als responsables de seguretat i a les persones treballadores d'aquestes entitats que tenen encomanades tasques en relació amb la configuració dels sistemes de tecnologies de la informació i la comunicació i sobre la seguretat de la informació a l'empresa, amb la voluntat de ser una eina per a la reflexió prèvia a la presa de decisions corporatives en aquest àmbit.

Aquesta Recomanació es complementa amb el *Manual de bon ús del correu electrònic*, que es publica de forma simultània amb aquesta Recomanació. El manual, que podreu trobar al web de l'Autoritat i descarregar-vos-el, s'adreça a totes les persones treballadores d'aquestes entitats que han d'emprar el correu electrònic per exercir les seves funcions, per tal que en el seu ús adoptin pràctiques que garanteixin el tractament adequat de la seva pròpia informació personal, com també de la privacitat de terceres persones.

L'objecte d'aquesta Recomanació, que no té caràcter normatiu, és, precisament, donar pautes perquè les empreses puguin regular i controlar l'ús del correu electrònic en l'àmbit laboral. Per això, s'hi inclouen recomanacions que puguin ajudar a difondre bones pràctiques i que contribueixin a oferir més seguretat i més respecte pels drets de les persones, en especial pel dret a la protecció de les dades de caràcter personal. I això cada organització ho ha de fer d'acord amb les seves necessitats a l'hora de tractar la informació de què és responsable. En aquesta tasca hi té un paper fonamental l'aprovació d'unes normes d'ús del correu electrònic.

En qualsevol cas, atès el caràcter canviant de la tecnologia i, en conseqüència, de la matèria objecte d'aquesta iniciativa, la present Recomanació no es concep com a quelcom estàtic, sinó més aviat com una eina dinàmica l'aplicació de la qual estarà sotmesa, per part de la mateixa Autoritat Catalana de Protecció de Dades, a un procés continuat de verificació, per comprovar-ne els resultats de la seva aplicació i adequar les previsions que s'hi contenen als nous problemes que es puguin plantejar.

I. El correu electrònic

1 Sistemes de correu electrònic

El correu electrònic és un sistema de missatgeria que permet la transmissió de missatges entre usuaris sense necessitat que estiguin connectats al mateix temps. Hi ha diferents aplicacions que permeten gestionar els missatges de correu electrònic, que es poden agrupar, bàsicament, en dues modalitats:

❑ Client de correu electrònic

Són programes (p. ex. Outlook, Outlook Express, Eudora, Mozilla Thunderbird, etc.) que serveixen per gestionar els missatges rebuts i per escriure'n de nous. El programa descarrega tots els missatges que s'emmagatzemen a l'ordinador, sens perjudici que determinats protocols (cas d'IMAP) puguin mantenir-los en el servidor. Es pot instal·lar en diferents dispositius (ordinador fix, portàtil, telèfon intel·ligent o *smartphone*, tauleta, etc...).

❑ Webmail o correu web

Hi ha sistemes de correu que s'identifiquen habitualment com a correu web o web mail. Amb independència que s'hi pugui accedir també a través d'un client de correu, es tracta d'un sistema d'accés a un servei de correu electrònic emprant el navegador d'Internet i el protocol http o https. Aquest sistema permet rebre i enviar correus des de qualsevol lloc, a través d'un web. Els missatges s'emmagatzemen al servidor on s'allotja el compte de correu.

Els servidors de correu web poden ser a tercers països, que potser no compten amb un nivell adequat de protecció de les dades de caràcter personal i, especialment en el cas del web mail, sovint les condicions les fixa i les modifica unilateralment el proveïdor. Si es tracta de serveis oferts gratuïtament, aquestes condicions sovint inclouen l'autorització per al tractament de la informació que s'hi conté amb finalitats publicitàries o altres finalitats. Sovint, també realitzen una anàlisi automàtica del contingut dels missatges enviats o rebuts. Aquesta anàlisi del contingut dels missatges pot ser útil, per exemple per detectar virus, però cal advertir que els proveïdors també la poden utilitzar per oferir, en la mateixa aplicació de correu, anuncis que hi estiguin relacionats.

Recomanacions

- ✓ Atribuir un compte de correu als treballadors que ho necessitin per exercir les seves funcions, ja sigui mitjançant el sistema de client de correu electrònic o de correu web. En aquest darrer cas, convé assegurar que l'empresa que facilita el correu tingui establertes polítiques de privacitat i seguretat adequades, a través de les corresponents clàusules contractuals vinculants per a totes les parts implicades.

2 L'adreça de correu electrònic

2.1 L'adreça de correu electrònic com a dada personal

L'adreça de correu electrònic és el conjunt de paraules o signes que identifiquen l'emissor o el receptor d'un missatge de correu electrònic. S'elabora a partir d'un conjunt de paraules o signes lliurement escollits, normalment, pel seu titular o per la organització a la qual pertany, amb l'únic límit que aquesta adreça no coincideixi amb la d'una altra persona. Està formada per una identificació de l'usuari, seguida del signe @ i, a continuació, el domini (identificació facilitada pel proveïdor del servei de correu, amb un punt, i unes sigles que poden identificar l'activitat de l'organització (p. ex. ".org") o les sigles del país (p. ex. ".es" o ".cat").

Es pot distingir:

❑ Adreces personalitzades

L'adreça conté directament informació sobre el seu titular: nom i cognoms, inicials, càrrec, número identificatiu, etc.

- ✓ Nom_Cognoms_@nom_del_domini
  joanidentitat@gencat.cat
- ✓ Inicials_@nom_del_domini
  E.C@gencat.cat
- ✓ Càrrec@nom_del_domini
  Directoraautoritat@gencat.cat
- ✓ Número identificatiu@nom_del_domini
  000000000857346@gencat.cat

En aquests casos, l'adreça de correu electrònic identifica directament al titular del compte i per tant s'ha de considerar com a dada de caràcter personal.

L'atribució d'una adreça de correu d'aquest tipus pot generar falses expectatives de privacitat, tant a la persona titular com a les persones que s'hi relacionen. Per això, en els casos en què es vulgui prohibir totalment la utilització del correu amb fins personals, pot ser convenient no atribuir una adreça de correu personalitzada.

❑ Adreces no personalitzades

Tot i que es tracta d'una adreça vinculada a un compte de correu d'una persona física determinada, l'adreça de correu electrònic no sembla contenir informació sobre el seu titular (empra una combinació alfanumèrica abstracta o sense cap significat):

Akatombe80@gmail.com

Abc123@terra.net

En aquests casos, l'adreça per si sola no identifica la persona que n'és titular. Però aquesta pot ser fàcilment identificable, sense un esforç desproporcionat, bé perquè l'adreça pot aparèixer juntament amb altres dades que en permeten la identificació, bé pel contingut del missatge, bé a través de les dades de què disposa el servidor de correu. Aquesta adreça també s'ha de considerar com a dada de caràcter personal.

❑ Adreces genèriques

L'adreça de correu electrònic respon a un compte genèric, d'ús compartit o d'una àrea de l'organització:

consultes@gencat.cat

En aquests casos, l'adreça de correu electrònic no es pot vincular a una persona física identificada o identificable, sinó que la poden atendre usuaris diferents. Per tant, no es pot considerar com a dada de caràcter personal. Amb una adreça d'aquest tipus desapareixen les expectatives de privacitat tant del mateix treballador com, especialment, de les persones que s'hi relacionen, atès que aquest compte de correu pot ser atès per usuaris diferents.

2.2 Publicació de l'adreça de correu electrònic a Internet/Intranet com a dada de contacte

La publicació de l'adreça de correu laboral o professional que es pugui associar a persones físiques constitueix una comunicació de dades de caràcter personal i, per tant, s'ha de subjectar al règim de comunicacions previst a la normativa de protecció de dades. Això vol dir que és necessari disposar del consentiment de la persona treballadora o d'una norma amb rang de llei que n'habiliti la comunicació.

En la mesura que la publicació de l'adreça de correu electrònic laboral o professional sigui necessària com a part del desplegament de les funcions que pot tenir atribuïdes un determinat lloc de treball, la seva difusió s'ha de considerar emparada a l'article 6.2 i 11.2.c) de la LOPD i a l'article 2.2 del RLOPD.

D'altra banda, en el cas de les llistes de persones pertanyents a grups de professionals, que tenen la consideració de fonts d'accés públic d'acord amb els articles 3.j) de la LOPD i 7 del RLOPD, l'adreça electrònica, que forma part de les dades incloses en aquesta font d'accés públic, es pot tractar per a la satisfacció d'un interès legítim perseguit pel responsable del fitxer o pel tercer a qui es comuniqui aquesta dada, sempre que no es vulnerin els drets i llibertats fonamentals de la persona afectada (art. 6.2 LOPD).

Recomanacions

- ✓ Establir comptes de correu vinculats a tràmits, serveis o àrees d'activitat, en lloc de persones determinades, sempre que sigui possible. Això pot ser especialment recomanable quan es faciliten comptes de correu a treballadors d'empreses externes que presten serveis de forma habitual dins l'empresa.
- ✓ Limitar la difusió de l'adreça electrònica de les persones treballadores a aquells supòsits en què resulti necessari per a les funcions atribuïdes a cadascuna d'elles. En la resta de supòsits, publicar l'adreça de correu electrònic només a la Intranet.
- ✓ Incorporar al lloc on es difonguin les adreces, un recordatori dels usos admesos d'aquestes adreces.
- ✓ Incorporar mecanismes per evitar la indexació de les adreces de correu, quan es publiquin al web, per evitar que es puguin utilitzar per a enviaments massius de correus electrònics. En aquest sentit, pot ser recomanable no incloure en la visualització de les pàgines l'adreça de correu, sinó només un enllaç que, en clicar-lo, sí que permeti accedir a una pàgina que incorpora una instrucció de no-indexació, que conté l'adreça. D'aquesta manera es pot permetre indexar el contingut de la pàgina inicial que conté l'enllaç, sense indexar-ne l'adreça.
- ✓ No utilitzar, ni cedir a terceres persones, les adreces de correu que formen part del directori corporatiu, per a finalitats diferents d'aquelles que resultin necessàries per desenvolupar les funcions encomanades a l'empresa.

3 El contingut del correu electrònic

En un correu electrònic hi figura diversa informació que es pot considerar com a dada de caràcter personal, en la mesura que ens ofereixi informació sobre una persona física identificable:

❑ Adreça de correu de l'emissor i el destinatari o destinataris

L'adreça de correu es pot vincular fàcilment a una persona física. En ocasions, la mateixa adreça ja en facilita la identificació. En altres casos, en el camp corresponent a l'adreça, juntament amb ella, o fins i tot substituint-la, hi apareix la identificació de la persona que n'és titular.

❑ Assumpte sobre el qual versa el correu

Convé que l'assumpte descrigui de forma concisa la naturalesa o el contingut del missatge i, si és possible, s'eviti incloure-hi dades de caràcter personal.

El grau de confidencialitat de les dades que s'hi incloguin serà menor que el de la informació que conté el cos del missatge, atès que la simple visualització de la safata d'entrada o sortida permet llegir l'assumpte.

❑ Data i hora del correu

La data i l'hora del correu també constitueixen una dada personal, atès que permeten establir el moment en què s'envia i, fins i tot, poden arribar a permetre establir el lloc on era una persona.

❑ Cos del missatge

És el contingut del missatge. Pot consistir en un text, amb format o sense, o en imatges, que poden contenir dades de caràcter personal. També pot contenir enllaços a pàgines web o documents que continguin dades personals.

❑ Peu de signatura

És el text que apareix a sota de la identificació de qui subscriu el missatge. Normalment, ofereix informació sobre el càrrec i l'organització a la qual pertany l'emissor.

Sovint, els sistemes de correu electrònic ofereixen la possibilitat d'incorporar en els missatges de correu un peu de signatura de forma automàtica.

❑ Documents adjunts

El correu electrònic permet adjuntar al missatge imatges, documents, vídeos o àudio. El volum d'informació personal que poden incloure els documents adjunts pot ser molt gran, per la qual cosa, per evitar revelacions indegudes d'informació, convé extremar la prudència a l'hora d'adjuntar fitxers. A més, cal vetllar per la seguretat d'aquestes dades i, si escau, valorar l'ús de mitjans tècnics, com ara tècniques de xifratge, per assegurar que el contingut no serà interceptat per tercers.

II. L'ús del correu electrònic

1 Normes d'ús del correu electrònic

Per tal d'evitar una mala utilització del correu electrònic que pugui perjudicar la seguretat de la informació que es tracta, l'empresa ha d'establir i posar en coneixement dels seus treballadors les normes d'ús del correu electrònic i definir les condicions en què, si escau, aquesta eina es pot utilitzar amb finalitats privades.

L'establiment, mitjançant aquestes normes, d'una política d'ús del correu ha de permetre a les persones treballadores conèixer amb seguretat el nivell de confidencialitat que poden esperar en l'ús d'aquestes tecnologies.

La manca d'una política adequada d'ús del correu electrònic, en canvi, pot produir, en la persona treballadora o en tercers, una expectativa de confidencialitat que pot donar lloc a situacions conflictives.

En la seva elaboració, convé comptar, sempre que sigui possible, amb la participació dels representants de les persones treballadores.

S'ha d'informar les persones treballadores de l'existència d'aquestes normes. A banda de fer-ne difusió a la intranet de l'empresa, per garantir que totes les persones treballadores en tinguin coneixement, es poden incorporar, com a annex, als contractes laborals, poden formar part del manual de benvinguda o poden adoptar la forma de circulars o instruccions comunicades als treballadors.

A banda de la seva participació en l'elaboració d'aquestes normes, també convé informar els representants de les persones treballadores de les normes que s'aprovin.

L'empresa ha de formar els seus treballadors en l'ús del correu electrònic i, especialment, en el coneixement de les opcions de privadesa que ofereixi el sistema emprat per l'empresa.

Aquestes normes s'han d'actualitzar d'acord amb l'evolució de la tecnologia disponible, de l'activitat de l'empresa i de les necessitats de les persones treballadores.

En aquestes normes s'haurien de tractar, com a mínim, els aspectes següents:

- ❑ Objecte i finalitat del document.
- ❑ Especificacions del sistema de correu electrònic (equips i programari).
- ❑ Instruccions generals d'ús del correu electrònic.
- ❑ Usos admesos i usos no admesos del correu electrònic professional i, si escau, del compte de correu personal facilitat per l'empresa. Cas d'admetre's un cert ús privat, convé determinar les condicions d'aquest ús (grau d'utilització amb finalitats privades, identificació dels missatges privats, emmagatzematge, eliminació del peu de signatura en els missatge privats, etc.).

- ❑ Usos admesos dels suports i dispositius mòbils o portàtils facilitats per l'empresa que permetin accedir al correu electrònic.
- ❑ Possibilitat o no d'emprar sistemes de correu web en el lloc de treball, ja sigui amb finalitats professionals o estrictament personals, o de rebre en el compte client corporatiu missatges d'altres comptes.
- ❑ Aspectes relatius al contingut dels missatges: encapçalaments, aspectes formals, llenguatge, avisos legals, peus de signatura, mida màxima dels arxius, etc.
- ❑ Usos admesos de les adreces publicades al directori de l'empresa.
- ❑ Mesures de seguretat aplicables:
  - Mesures d'identificació i autenticació d'usuaris: assignació de claus i política de contrasenyes.
  - Mesures que han d'adoptar les persones treballadores per garantir la confidencialitat de la informació i, si escau, el secret professional.
  - Procediment per autoritzar la transmissió de dades a través de la xarxa.
  - Utilització de la signatura electrònica i mecanismes de xifratge.
  - Protocol a seguir per les persones treballadores, i per la mateixa empresa, en cas que es produeixi alguna incidència en l'ús del correu.
  - Altres mesures de seguretat.
- ❑ Períodes de conservació de la informació a les carpetes d'entrada, d'elements enviats i a la paperera, en sistemes de client de correu.
- ❑ Informacions que s'han de conservar durant un període més llarg en forma centralitzada o bé, per exemple, en còpies de seguretat, per a la gestió tècnica de la xarxa o arxius "log".
- ❑ Solucions per garantir la continuïtat de l'activitat en cas d'absència de la persona treballadora, amb especial referència als missatges de resposta automàtica.
- ❑ Tractament que cal donar als missatges inadequats que es rebin.
- ❑ Mesures de control de l'ús de correu que pot dur a terme l'empresa:
  - Mecanismes de filtratge.
  - Programes i dispositius de control i monitorització, si estan justificats
  - Supòsits i procediment d'accés als comptes de correu per part de l'empresa.
- ❑ Conseqüències per a la persona treballadora de l'ús indegut del correu electrònic.
- ❑ Altres normes de bon ús del correu electrònic adreçades a les persones treballadores o normes de comportament general a la xarxa o *netiquettes*. Amb aquesta finalitat, aquesta Autoritat ha publicat també el *Manual de bon ús del correu electrònic*, adreçat específicament als treballadors usuaris dels sistemes de correu electrònic.

A l'Annex I d'aquesta Recomanació s'ofereix un model de normes d'ús del correu electrònic a l'àmbit laboral, que es pot utilitzar per elaborar les normes de cada empresa. Convé adequar aquest model a les necessitats de cada organització, pel que fa al tractament de la informació.

2 Els mecanismes d'identificació i autenticació

❑ Identificació

Procediment per conèixer la identitat d'un usuari, en aquest cas de l'usuari de correu electrònic. Amb aquesta finalitat, s'assigna un nom a cada usuari.

❑ Autenticació

Procediment de comprovació de la identitat d'un usuari. En un sistema de correu, això es fa normalment a través de la introducció d'una contrasenya o *password* a més de la identificació de l'usuari, tot i que també es poden emprar altres sistemes, com ara un certificat digital.

❑ Contrasenya

Informació confidencial, constituïda per una cadena de caràcters. La robustesa d'aquesta contrasenya depèn de les característiques exigides per a establir-la (política de contrasenyes). Una contrasenya es pot considerar forta si:

- Té una longitud mínima de 8 caràcters.
- S'ha triat a l'atzar i no es pot trobar a cap diccionari.
- Només la pot deduir el mateix usuari.
- Requereix esforços desproporcionats esbrinar-la.
- Inclou lletres, números, majúscules i minúscules i, si el sistema ho permet, símbols.

En canvi, es pot considerar que una contrasenya és dèbil si:

- Identifica fàcilment l'usuari.
- Conté menys de 8 caràcters.
- Ve predeterminada pel sistema o per l'administrador del sistema.
- És fàcilment identificable utilitzant diccionaris o bé consisteix en noms propis, dates significatives, números coneguts o variacions simples d'aquestes paraules.

D'altra banda, en el cas d'oblit de la contrasenya, alguns programes permeten recuperar-la o modificar-la contestant una pregunta establerta per la mateixa persona usuària. De la complexitat de la resposta a aquesta pregunta també en depèn la robustesa de la contrasenya.

L'empresa ha d'establir, en les normes d'ús del correu electrònic, una política de contrasenyes adequada per garantir la identificació inequívoca i personalitzada de qualsevol usuari.

Recomanacions

- ✓ Establir, per a l'accés al compte de correu, un mecanisme que garanteixi la identificació de forma inequívoca i personalitzada de qualsevol usuari i la seva autenticació mitjançant una contrasenya forta.
- ✓ No crear usuaris que s'identifiquin amb l'adreça de correu, atès que facilitaria la identitat de l'usuari i donaria a un tercer la possibilitat de bloquejar el compte.
- ✓ Emmagatzemar els usuaris i les contrasenyes, o si més no les contrasenyes, de forma inintel·ligible, utilitzant tècniques de xifratge.

- ✓ Mantenir la confidencialitat de l'usuari i la contrasenya atribuïts quan es comuniquen per primera vegada a l'usuari.
- ✓ Evitar riscos quan es trameten les contrasenyes al servidor de correu, utilitzant sistemes de transmissió segura, com ara el xifratge.
- ✓ Establir la periodicitat amb què s'ha de modificar la contrasenya, que en cap cas ha de ser superior a un any.
- ✓ No permetre, en cas de canvi periòdic de la contrasenya, que es repeteixin les darreres contrasenyes utilitzades.
- ✓ Prohibir expressament l'ús no autoritzat del correu electrònic d'altres usuaris mitjançant l'intercanvi d'usuaris o usuaris compartits.
- ✓ Instal·lar sistemes de blocatge a l'ordinador que es puguin activar fàcilment en cas d'absència o que obliguin a l'usuari a tornar a introduir la seva contrasenya després d'un determinat període d'inactivitat.
- ✓ Informar els usuaris del següent:
  - Les seves obligacions en relació amb la conservació de les contrasenyes i els períodes de modificació.
  - El caràcter personal i no transferible dels usuaris i contrasenyes.
  - Les responsabilitats en què es pot incórrer per la pèrdua, alteració fraudulenta o suplantació en els sistemes d'autenticació.
- ✓ Establir un protocol adequat per retirar els permisos d'accés, quan un treballador deixa de prestar serveis a l'entitat.

3 Seguretat de les comunicacions

La utilització del correu electrònic, per si sola, no garanteix l'autenticitat ni la integritat de la comunicació. És a dir, no garanteix l'autenticitat de la identitat de qui apareix com a emissor ni que el contingut emès coincideixi amb el contingut rebut. Això pot generar problemes tant pel que fa a la suplantació de la identitat com pel que fa a l'alteració dels missatges i arxius adjunts.

Per garantir l'autenticitat i la integritat de les comunicacions, es pot utilitzar la signatura electrònica.

❑ Signatura electrònica

La signatura electrònica és un conjunt de dades en forma electrònica que, consignades o associades amb altres, es poden utilitzar com a mitjà d'identificació de la persona que signa, mitjançant un sistema de criptografia asimètrica. Aquest mecanisme permet autenticar l'emissor i la integritat del missatge.

La signatura electrònica es pot generar a partir d'un certificat electrònic, això és, un document signat electrònicament per un prestador de serveis de certificació, que vincula unes dades de verificació de signatura a un signant i en confirma la identitat.

Cada administració, amb la col·laboració, si escau, de l'Agència Catalana de Certificació, ha de proveir el seu personal de sistemes de firma electrònica, que poden identificar de forma conjunta el titular del lloc de treball o càrrec i l'administració on presta serveis.

En el web de l'Autoritat Catalana de Protecció de Dades, podeu trobar informació sobre com utilitzar la signatura electrònica en diferents sistemes de correu electrònic.

D'altra banda, cal assegurar també la confidencialitat de la informació transmesa, és a dir que només hi tinguin accés les persones adequades.

❑ Xifratge

Per garantir la confidencialitat de les comunicacions, es pot utilitzar el xifratge.

El xifratge consisteix en la transformació d'un missatge, fent servir una clau per evitar que qui no la conegui el pugui interpretar

És obligatori emprar mecanismes de xifratge de les dades o bé qualsevol altre mecanisme que garanteixi que la informació no sigui intel·ligible ni manipulada per tercers, en la transmissió de dades de caràcter personal a través de xarxes públiques o xarxes sense fil de comunicacions electròniques de dades, quan el tractament requereixi l'aplicació de mesures de seguretat de nivell alt:

- Dades d'ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual.
- Dades obtingudes amb fins policials sense el consentiment de les persones afectades.
- Dades derivades d'actes de violència de gènere.

En el web de l'Autoritat Catalana de Protecció de Dades, podeu trobar informació sobre com utilitzar el xifratge en diferents sistemes de correu electrònic.

El sistema de correu ha de garantir la seguretat de la informació vinculada a la seva utilització. En aquest sentit, cal tenir en compte que la sortida d'informació de caràcter personal per mitjà del correu electrònic, ja sigui en el text del missatge o en els fitxers adjunts, l'ha d'autoritzar el responsable del fitxer o ha d'estar degudament autoritzada en el document de seguretat.

També convé tenir en compte que algunes pàgines web o correus electrònics poden incorporar *web bugs* (petites imatges incrustades que poden donar informació sobre la nostra adreça IP i sobre el nostre accés al correu) o hipervincles invisibles que permeten transmetre l'adreça de correu electrònic a un tercer.

L'empresa ha de preveure, en el protocol inclòs a les normes d'ús del correu electrònic, que les persones treballadores que detectin algun tipus d'incidència, o bé dubtin sobre la seguretat del sistema, ho comuniquin immediatament al responsable de seguretat, amb una breu descripció de l'incident i la data i hora en què s'hagi detectat, perquè es resolgui la incidència i/o es revisi el funcionament del seu correu electrònic.

Recomanacions

- ✓ Establir per defecte una configuració de seguretat en els equips i programes de correu adequada a la naturalesa de les dades més sensibles que es prevegi que es tractaran.
- ✓ Protegir sempre l'accés a la bústia de correu amb un sistema que garanteixi la identificació i l'autenticació, especialment quan es rep en dispositius mòbils.
- ✓ Orientar les pantalles dels terminals de manera que es preservi el contingut dels missatges respecte de terceres persones que es puguin trobar a les dependències on és el lloc de treball.
- ✓ Configurar els dispositius mòbils perquè es bloquegin automàticament per tal que, en cas de pèrdua, cap altra persona pugui accedir als missatges de correu electrònic.
- ✓ Prohibir la instal·lació de programari no autoritzat per l'empresa.
- ✓ Instal·lar programari antivirus, filtres antiinundació o *anti-spam* o altres mecanismes per reduir la recepció de missatges no sol·licitats.
- ✓ Requerir al proveïdor que la comunicació entre el dispositiu d'accés al correu i el servidor estigui xifrada.
- ✓ Demanar que s'eliminin, de forma immediata, els missatges que puguin contenir virus o *malware* o programari maliciós. L'esborrat complet requereix eliminar-los també de la paperera de reciclatge.
- ✓ Establir un sistema adequat de resolució de qualsevol incidència de seguretat que es detecti en el sistema.
- ✓ Incloure a les normes d'ús del correu instruccions sobre l'ús de la signatura electrònica i el xifratge dels missatges.
- ✓ Formar el personal en la utilització dels instruments de signatura electrònica i xifratge dels missatges.

4 Ús del correu amb finalitats privades

El desenvolupament de les funcions atribuïdes a molts llocs de treball fa indispensable l'atribució d'un compte de correu electrònic per poder dur a terme d'una forma eficaç les funcions encomanades. Sovint, però, pot resultar difícil separar d'una forma hermètica la vida privada de les persones treballadores respecte de la seva activitat professional. I això no només per l'actuació de la persona treballadora, sinó també per necessitats de la mateixa empresa i perquè a més, la persona treballadora no sempre pot controlar els missatges que rep al seu compte de correu. Això és especialment evident en el cas de dispositius mòbils o sistemes d'accés remot establerts, precisament, per poder accedir a aquests mitjans fora del lloc de treball i de l'horari laboral.

Això permet distingir entre diferents tipus de comptes de correu, d'acord amb la seva finalitat:

- **Compte corporatiu per a ús laboral:** és propietat de l'empresa o institució en la qual es presta serveis, que en determina tant l'usuari com el proveïdor i el domini, i també les finalitats i condicions d'ús a què està sotmès. L'atribució d'aquest compte de correu es fa per motius estrictament laborals.

- **Compte corporatiu per a ús privat:** l'empresa pot atribuir al treballador un compte de correu electrònic per a ús estrictament particular. En podrà limitar l'ús, però no controlar-ne el contingut.

- **Compte privat o personal:** el proporciona algun proveïdor de serveis, sigui de manera gratuïta o mitjançant pagament, o l'empresa o institució en la qual es presta serveis. Aquest correu és d'ús estrictament personal.

L'atribució del compte de correu qualificat com a corporatiu o laboral obeeix a motius estrictament laborals. No obstant això, tal com s'ha exposat, atesa la dificultat en molts casos de separar la vida privada de l'activitat laboral, i llevat que l'empresa estableixi expressament el contrari, hi ha una certa acceptació social respecte de la possibilitat d'emprar aquests mitjans per a finalitats privades.

Convé, però, que en les normes d'ús del correu electrònic l'empresa estableixi si l'ús privatiu d'aquest mitjà és admissible, i en quina mesura (horari, volum dels missatges enviats o rebuts, etc.).

Quan sigui admissible una certa utilització del correu amb fins privats, una actuació diligent de la persona treballadora permet assegurar el respecte a la seva privacitat. A aquest efecte, resulta fonamental limitar la difusió de l'adreça de correu professional a finalitats estrictament professionals, configurar els missatges de forma adequada, organitzar-los i verificar periòdicament els que s'han d'eliminar.

D'altra banda, per fer compatibles la prohibició d'utilitzar el correu laboral amb finalitats privades i el desenvolupament de la vida privada de les persones, quan les circumstàncies ho aconsellin, pot ser recomanable atribuir no només un compte corporatiu o laboral sinó també un compte privat o personal, per tal d'evitar, o com a mínim reduir, la utilització d'un mateix compte amb finalitats diverses. L'atribució d'aquest correu personal pot substituir-se per una autorització per utilitzar algun sistema de correu web, amb els límits que estableixi la mateixa empresa.

Convé també, si escau, informar les altres persones que previsiblement pugui relacionar-s'hi sobre el caràcter exclusivament professional de les adreces de correu electrònic (p.ex. a través de la inserció d'un avís en tots els missatges sortints de l'organització, o amb un avís en el directori corporatiu).

En qualsevol cas, l'assignació d'una adreça de correu que no incorpori dades vinculades a una persona concreta pot facilitar que terceres persones percebin el caràcter exclusivament professional del compte de correu.

Quan, en cas d'absència, la continuïtat del servei requereixi redireccionar els missatges que arribin a un determinat compte de correu al compte de correu d'una altra persona treballadora, convé advertir amb antel·lació suficient la persona afectada, perquè pugui adoptar les mesures adients i, si escau, advertir d'aquest fet els seus contactes.

Recomanacions

- ✓ Establir, a les normes d'ús del correu, si les persones treballadores poden utilitzar el compte de correu professional amb finalitats personals.
- ✓ Admetre l'ús a l'àmbit laboral d'un sistema de correu via web per a finalitats privades, concertat per la mateixa persona interessada i amb els límits establerts a les normes d'ús del correu electrònic de l'empresa.

Cas que s'admeti la utilització del compte de correu professional amb finalitats personals:

Recomanacions

- ✓ Establir, a les normes d'ús del correu electrònic, un període màxim de conservació dels missatges privats. Si les persones treballadores no han esborrat abans els missatges que siguin innecessaris, o els han reenviat a un compte de correu privat, en complir-se aquest termini, els missatges d'aquesta naturalesa s'han d'esborrar.
- ✓ Establir les normes d'ús dels dispositius mòbils amb accés al correu electrònic, com ara telèfons intel·ligents o *smartphones* o ordinadors portàtils, fora de l'horari laboral.
- ✓ Crear carpetes per emmagatzemar els correus identificats com a "privats" o "personals". Això es pot fer de manera automàtica, mitjançant filtres a partir del seu origen o que incloguin aquestes expressions o d'altres preestablertes a l'assumpte del missatge, o manualment a partir de la decisió del titular del compte de correu.

5 Ús del correu amb finalitats sindicals

La llibertat d'informació és un element essencial del dret fonamental a la llibertat sindical. Tot i que la legislació laboral no preveu expressament, per a l'exercici d'aquest dret, l'ús dels mitjans tecnològics que l'empresa posa a disposició de les persones treballadores per a desenvolupar les seves funcions, els representants de les persones treballadores poden exercir aquest dret mitjançant l'ús de les tecnologies de la informació i la comunicació, sempre que això no afecti el desplegament normal de l'activitat empresarial.

No hi ha una previsió legal expressa de facilitar la transmissió d'informació sindical als treballadors, afiliats o no, per mitjà d'un sistema de correu electrònic a càrrec de l'empresa. Això no obstant, si l'empresa disposa d'aquest mitjà, els representants de les persones treballadores poden emprar-lo per transmetre notícies d'interès sindical als seus afiliats i a la resta de treballadors de l'empresa, d'acord amb les normes d'ús del correu electrònic de l'empresa.

En qualsevol cas, l'ús del correu electrònic proporcionat per l'empresa per part dels representants de les persones treballadores amb aquesta finalitat està subjecte, d'acord amb la doctrina constitucional establerta, a una sèrie de límits:

- No es pot excloure la utilització del correu electrònic amb aquesta finalitat en termes absoluts.
- La comunicació no ha de pertorbar l'activitat normal de l'empresa.
- El seu ús no pot comportar gravàmens o costos addicionals per a l'empresa.

Amb aquesta mateixa finalitat, els representants sindicals també poden emprar, sense consentiment de les persones interessades, les adreces que figurin al directori de l'empresa.

En qualsevol cas, els treballadors poden exercir el seu dret d'oposició a la utilització de la seva adreça de correu electrònic amb aquesta finalitat davant del responsable del fitxer.

Recomanacions

- ✓ Autoritzar l'ús del correu electrònic com a instrument de comunicació i informació entre sindicats i treballadors, amb garantia d'inviolabilitat de les comunicacions d'acord amb el marc legal vigent, sempre que l'activitat i les característiques generals de l'empresa ho permetin. No obstant això, convé valorar la possibilitat de difondre la informació sindical entre les persones treballadores, mitjançant sistemes que permetin fer-ho sense necessitat de recollir la dada del correu de les persones treballadores, com per exemple:
- ✓ Emprar llistes de distribució que permetin que el sindicat remeti la informació sense accés a les dades.
- ✓ Posar una finestreta d'informació sindical a disposició de les persones treballadores, a la intranet corporativa.
- ✓ Establir un procediment fàcil per a l'exercici, davant el sindicat i/o el responsable del fitxer, del dret d'oposició a la utilització de l'adreça electrònica amb aquesta finalitat.
- ✓ Informar els treballadors de la possibilitat d'exercir aquest dret, en el moment que es facilitin les dades als representants dels treballadors, llevat que ja se'ls hagi informat abans. Això sens perjudici que el representant sindical també n'informi degudament els treballadors.

III. L'accés al correu electrònic per part de l'empresa

Les consideracions contingudes en aquest apartat es refereixen no només als comptes de correu en què les normes d'ús de l'empresa n'admeten un cert ús privat, sinó també respecte dels comptes de correu respecte dels quals s'estableixi un ús exclusivament professional, atès que amb independència de l'ús que en faci el mateix treballador, aquest no sempre pot evitar l'ús que en facin terceres persones per remetre-li missatges de caràcter personal.

L'empresa només pot accedir als comptes de correu electrònic corporatiu facilitats als seus treballadors quan l'accés estigui justificat i no hi hagi cap altre mecanisme que permeti assolir l'objectiu perseguit sense necessitat d'accedir-hi.

El mitjà i l'abast del control ha de ser proporcionat a la finalitat que es persegueixi. Per això, si és possible, s'ha de limitar a les dades sobre l'emissor i el receptor, l'hora de la comunicació i altres dades com ara el nombre de missatges enviats, el volum d'informació o el tipus d'arxius que s'hagi adjuntat o altres sistemes d'anàlisi automatitzada dels missatges entrants i sortints que no n'analitzin el contingut. Només si aquesta informació no és suficient per assolir la finalitat perseguida, es podrà accedir al contingut dels missatges sempre que es compleixin les garanties escaients, evitant entrar en els missatges que es puguin identificar com a privats. En el cas que un missatge d'aquesta naturalesa s'obri per error, cal tancar-lo tan bon punt es pugui constatar la seva naturalesa privada.

Aquest accés s'ha de dur a terme d'acord amb les normes d'ús del correu electrònic que aprovi l'empresa, que han d'advertir sobre els mecanismes de control de l'ús de les tecnologies que puguin afectar la privacitat de les persones, les conseqüències que es poden derivar del control i les garanties per a les persones treballadores, en especial el dret a ser-ne informat.

S'ha d'informar tant l'administrador del sistema com la resta de persones que intervinguin en les operacions de control dels seus deures i obligacions en matèria de seguretat, i en especial del deure de secret. Sens perjudici de l'obligació general de secret que es deriva de la normativa de protecció de dades, pot ser convenient fer signar a les persones que intervenen en aquestes operacions un compromís de confidencialitat respecte de les dades a què tinguin accés.

L'accés que es dugui a terme en qualsevol dels supòsits descrits ha de quedar degudament reflectit en el registre d'incidències.

Les persones treballadores poden exercir els seus drets d'accés, rectificació, cancel·lació i oposició respecte de la informació que hagi obtingut l'empresa mitjançant les mesures de control implantades.

L'accés s'ha de limitar a la informació que resulti indispensable per assolir algun dels objectius següents:

1 Accés per realitzar tasques de manteniment del correu electrònic

L'accés als comptes de correu electrònic corporatiu per a les tasques de manteniment, el suport tècnic o la seguretat del sistema no ha de comportar l'accés al contingut dels missatges. Es pot dur a terme tenint en compte:

- ❑ Aquestes operacions només les pot fer el personal autoritzat pel responsable de seguretat.
- ❑ S'ha d'informar les persones treballadores afectades sobre les tasques que cal fer i les persones que les executaran, com també de la possibilitat de ser presents durant l'accés.
- ❑ Un cop finalitzades les tasques de manteniment o de suport tècnic, convé elaborar un informe de les tasques fetes i, si s'ha detectat alguna anomalia, anotar-la al registre d'incidències i comunicar-la a l'òrgan competent.

2 Accés per garantir la continuïtat de l'activitat en absència de la persona treballadora (vacances, malaltia, etc.)

L'absència d'un treballador, especialment si és de llarga durada, pot comportar problemes per a la continuïtat de l'activitat normal de l'empresa, si no es pot accedir a un determinat compte de correu. Per això és convenient, si és possible, planificar les mesures que s'adoptaran per garantir la continuïtat durant l'absència (p. ex. la persona treballadora pot eliminar o traslladar tots els missatges personals i autoritzar l'accés a un altre treballador, adoptant els canvis pertinents, tant a l'inici com a la fi del període, pel que fa al canvi de les contrasenyes).

Si això no és possible, cal tenir en compte:

- ❑ L'òrgan superior de la persona treballadora absent ha de valorar de forma motivada la necessitat de la intervenció per a la continuïtat del servei.
- ❑ L'accés al compte de correu electrònic s'ha de comunicar a la persona treballadora amb suficient antelació. Si no fos possible aquesta comunicació prèvia, s'ha de fer posteriorment, tan aviat com sigui possible.
- ❑ Convé accedir-hi sota la supervisió de l'òrgan superior de la persona treballadora i, cas que se li hagi pogut comunicar, amb la seva assistència o de la persona que designi, si ho desitja.
- ❑ No es pot accedir, per aquest motiu, als missatges que es puguin identificar clarament com a privats o personals.

3 Accés quan hi hagi indicis d'un possible mal ús

Per raons de seguretat, l'empresa pot monitoritzar el trànsit de correu electrònic (nombre de missatges, volum de missatges o fitxers adjunts etc.), sense entrar a analitzar-ne el contingut. Aquesta monitorització pot ser sistemàtica o aleatòria, sense que en cap cas pugui ser discriminatòria.

Si hi ha indicis d'un mal ús del correu per part de la persona treballadora, per incomplir les normes que hagi aprovat l'empresa, s'ha de posar en coneixement de la persona treballadora, llevat que això pugui obstaculitzar les investigacions escaients. Quan aquest mal ús pugui ser constitutiu de delicte o falta, s'ha de comunicar al ministeri fiscal. En qualsevol d'aquests casos pot donar lloc a una informació reservada o a un procediment disciplinari, en el si del qual es poden adoptar les mesures que estiguin a l'abast per solucionar el problema, que poden incloure el bloqueig dels missatges.

En aquest accés, que ha de ser proporcionat al tipus de risc que es pugui derivar del mal ús del correu per a l'empresa o terceres persones, convé tenir en compte:

- ❑ L'accés l'ha de dur a terme la persona designada pel responsable de seguretat, en presència de la persona treballadora o, si això no és possible, del representant del personal i de la persona instructora o inspectora.
- ❑ Un cop s'hi ha accedit, convé elaborar un informe de les actuacions realitzades i dels resultats obtinguts i incorporar-lo, si escau, a l'expedient corresponent.

4 Cessament de la relació laboral de la persona treballadora amb l'empresa

Quan una persona treballadora deixi de prestar serveis a l'empresa, l'òrgan competent en matèria de gestió de personal ha de comunicar-ho immediatament al responsable de seguretat per tal que s'inutilitzin els codis d'usuari i les contrasenyes del treballador i, si escau, s'inclogui un missatge automàtic de resposta per al correu entrant que indiqui la nova adreça a la qual es poden adreçar els missatges per raons professionals.

L'empresa ha de facilitar a la persona treballadora l'obtenció dels missatges privats del compte de correu, sempre que no superin el període màxim de conservació establert a les normes d'ús del correu per als missatges d'aquesta naturalesa. En aquest cas, s'hi accedirà en presència de la persona treballadora, per tal d'identificar els missatges de caràcter exclusivament personal.

Els missatges es poden esborrar o transferir a un altre compte de correu, un cop hagi transcorregut el termini atorgat a la persona treballadora sense que hagi manifestat la intenció d'emportar-se o de destruir els missatges privats que s'hi contenien.

En cas de defunció de la persona treballadora, els missatges personals es poden esborrar, sens perjudici que es mantinguin, degudament bloquejats, si les circumstàncies ho aconsellen.