Manual de bon ús del correu electrònic

Guia per a les persones treballadores per a la protecció de la privacitat en l'ús del correu electrònic

apdcat
Autoritat Catalana de Protecció de Dades

Generalitat de Catalunya

Índex

Tutorial annex

Com signar i xifrar un missatge de correu electrònic

Correu electrònic

☐ DEFINICIONS

Correu electrònic:	sistema de missatgeria que permet la transmissió de missatges entre usuaris, sense necessitat que estiguin connectats al mateix temps.
Adreça de correu:	conjunt de paraules o signes que identifiquen l'emissor o el receptor d'un missatge de correu electrònic.
Usuari:	persona que utilitza els mitjans informàtics, en aquest cas el correu electrònic.
Compte de correu o bústia de correu:	espai facilitat per un proveïdor de correu electrònic, on s'envien, reben o emmagatzemen els missatges de correu electrònic.
Proveïdor de correu:	empresa que ofereix el servei de correu electrònic. El proveïdor assigna una adreça de correu, a la qual es pot accedir per mitjà d'un nom d'usuari i una contrasenya.
Adreça IP:	número que permet identificar els dispositius dins d'una xarxa que utilitza el protocol IP, com ara Internet.
Empresa:	en aquesta Guia, s'utilitza el terme *empresa* per a referir-se a totes les entitats incloses dins l'àmbit d'actuació de l'APDCAT.

Què és una adreça de correu electrònic?

És el conjunt de paraules o signes que identifiquen una bústia a la qual o des de la qual s'envien missatges de correu electrònic. S'elabora a partir d'un conjunt de signes o paraules lliurement escollits:

L'adreça de correu electrònic és una dada de caràcter personal?

És dada personal

☐ Adreces personalitzades

L'adreça de correu electrònic identifica directament la persona titular del compte (amb el nom i els cognoms, les inicials, el càrrec, un número identificatiu, etc.) i, per tant, s'ha de considerar com a dada de caràcter personal.

joanidentitat@gencat.cat
E.C@gencat.cat
Directora@gencat.cat
000000000857346@gencat.cat

Atenció!

Que una adreça sigui personalitzada no vol dir que el correu es pugui utilitzar per a finalitats privades. Cal consultar les normes d'ús del correu corporatiu, per conèixer si n'està permesa la utilització amb fins personals.

☐ Adreces no personalitzades

En aquest cas, l'adreça de correu no identifica directament la persona titular del compte de correu:

Akatombe80@gmail.com
Abc123@terra.net

Encara que l'adreça per si sola no identifica la persona que n'és titular (empra una combinació alfanumèrica abstracta o sense cap significat), aquesta pot ser fàcilment identificable.

- perquè l'adreça pot aparèixer juntament amb altres dades que en permeten la identificació.
- pel contingut del missatge.
- a través de les dades de què disposa el servidor de correu, sense un esforç desproporcionat.

No és dada personal

☐ Adreces genèriques

L'adreça de correu electrònic respon, per exemple, a un servei, una activitat o una àrea de l'organització:

consultes@gencat.cat

En aquests casos, la informació que ens ofereix l'adreça de correu electrònic no es pot vincular a una persona física identificada o identificable. Per tant, no es pot considerar com a dada de caràcter personal. Sovint la poden atendre usuaris diferents, prèviament determinats.

Atenció!

En els comptes vinculats a aquestes adreces, ni el treballador ni les persones que s'hi relacionen no poden tenir cap expectativa de privacitat.

☐ Poden publicar la meva adreça de correu professional al web corporatiu de la meva empresa, sense el meu consentiment?

Sí, amb finalitats estrictament professionals i només en els casos en què resulti necessari, d'acord amb les funcions que tingui atribuïdes el treballador. En cas contrari, l'adreça es podrà publicar només a la intranet.

Quins sistemes de correu electrònic podem fer servir?

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

☐ Client de correu electrònic

- Són programes que serveixen per gestionar els missatges rebuts i per escriure'n de nous (p. ex. Outlook, Outlook Express, Eudora, Mozilla Thunderbird, etc.).
- 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...).

Thunderbird reclaim your inbox. Outlook

☐ Webmail o correu web

- 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.
- 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 web.

Windows Live Hotmail · Gmail by Google · msn · YAHOO!

Atenció! Els servidors de correu poden ser a tercers països, que potser no compten amb un nivell adequat de protecció de les dades de caràcter personal, i sovint, especialment en el web mail, les condicions les fixa i les modifica unilateralment el proveïdor.

Quan es tracti de serveis oferts gratuïtament, recordeu que:

- Aquestes condicions acostumen a incloure l'autorització per al tractament de la informació que s'hi conté amb finalitats publicitàries o altres finalitats.
- Sovint els servidors 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, a més, sovint els proveïdors l'empren per oferir, en la mateixa aplicació de correu, anuncis relacionats amb el missatge de correu electrònic o d'altres circumstàncies relacionades amb la seva tramesa.

☐ Puc fer servir el correu amb finalitats privades?

- En els supòsits en què les normes d'ús del correu establertes per l'empresa n'admetin un cert ús privat, no en feu un ús abusiu.
- No faciliteu l'adreça de correu professional en tràmits personals.
- Feu constar en el títol dels missatges la naturalesa privat o personal del missatge o alguna altra expressió que permeti a l'empresa deduir-ne aquest caràcter, en el cas que aquesta hagi d'accedir al compte de correu.
- Elimineu, tan bon punt sigui possible, la informació privada emmagatzemada en els comptes de correu facilitats per l'empresa. Especialment, quan us absenteu del vostre lloc de treball per un període llarg (vacances, viatges, ingressos hospitalaris, etc.).
- Si sou representants sindicals a la vostra empresa, podeu fer-ne ús per difondre informació sindical a la resta de treballadors, sempre que no es pertorbi l'activitat normal de l'empresa.

☐ L'empresa pot accedir al meu correu electrònic?

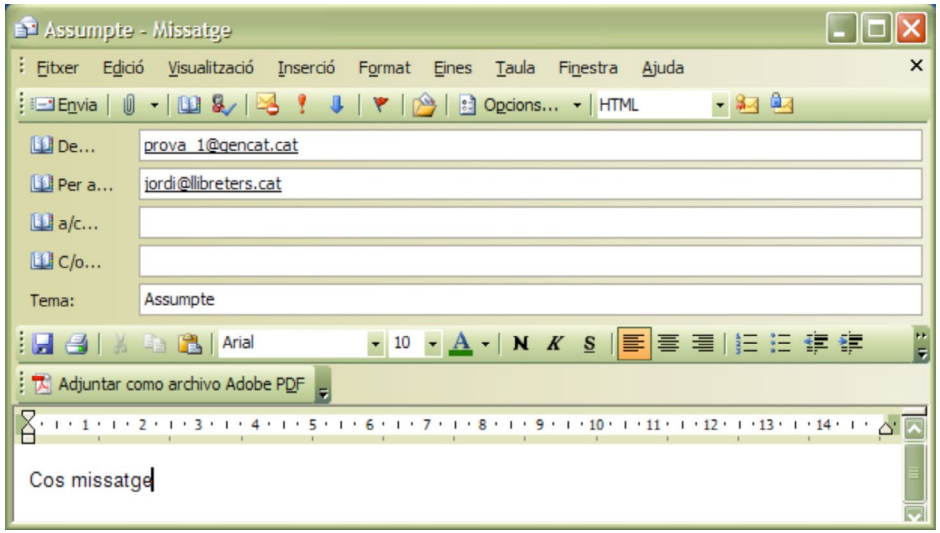
L'empresa només pot accedir als comptes de correu electrònic corporatiu facilitats als seus treballadors quan aquest accés estigui justificat i no hi hagi cap altre mecanisme que permeti assolir l'objectiu perseguit sense necessitat d'accedir-hi.

Aquest accés s'ha de dur a terme d'acord amb les normes d'ús del correu electrònic aprovades prèviament per 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 i les conseqüències que es poden derivar del mal ús.

Recordeu

- Consultar les normes d'ús del correu electrònic corporatiu per conèixer:
  - Si s'admet l'ús del correu professional assignat per a finalitats privades.
  - Si l'empresa facilitarà als treballadors un compte de correu per a ús privat.
  - Si l'empresa permet als treballadors utilitzar un compte de correu del propi treballador durant l'horari laboral per a finalitats privades.
- Cal evitar l'ús de comptes de correu per a comunicacions relacionades amb l'activitat pròpia de l'empresa, que no hagin estat proporcionats per proveïdors designats per l'empresa.

Quins elements formen un correu electrònic?



☐ Adreça de correu de l'emissor i del destinatari

Sovint, l'adreça de correu es pot vincular fàcilment a una persona física. En ocasions, la mateixa adreça ja en facilita la identificació. En altres, 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

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 poden constituir 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 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.

Recordeu

- Si es tracta d'un missatge de naturalesa privada, i això no es pot deduir de l'encapçalament, convé indicar-ho a l'assumpte.
- Eviteu incloure a l'assumpte informació personal, llevat que resulti estrictament necessari.
- Verifiqueu el contingut del correu electrònic, especialment dels fitxers adjunts, abans d'enviar-lo, per comprovar la identitat de les persones destinatàries, si les dades que hi figuren es poden transmetre i quines són les mesures de seguretat exigibles.
- Eviteu la comunicació de dades identificatives innecessàries, quan el contingut faci referència a terceres persones. En cas que no es pugui evitar la comunicació d'aquestes dades, es recomana fer-ho mitjançant un arxiu adjunt.
- Inhabiliteu l'opció de peu de signatura automàtic o, si escau, elimineu del peu de signatura la informació relativa al càrrec i l'organització on es presta els serveis, quan es tracti de missatges de correu per a finalitats privades.

Accés al correu: identificació i autenticació

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.

☐ Identificació

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

☐ 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 de la 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 ho permet el sistema, símbols.

Una **contrasenya** es pot considerar **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.

Recordeu

- Modifiqueu la contrasenya predeterminada pel sistema, quan hi accediu per primera vegada.
- Escolliu contrasenyes fortes. Una clau personal d'accés que sigui difícil de desxifrar és garantia de seguretat.
- Guardeu la contrasenya de forma segura. No la guardeu anotada en llocs de fàcil accés.
- Canvieu la contrasenya amb la periodicitat requerida pel sistema.
- Per als casos d'oblit de la contrasenya, quan s'hagi de respondre una pregunta per recuperar-la o modificar-la, eviteu preguntes que es puguin respondre amb una mínima investigació.
- Comuniqueu immediatament, seguint el procediment de gestió d'incidències establert, qualsevol incidència que en comprometi la seguretat.
- No faciliteu la contrasenya a terceres persones, encara que us la sol·licitin per fer proves al sistema o similars.
- No trieu l'opció de recordar la contrasenya.
- Tanqueu la sessió del correu electrònic o bloquegeu l'ordinador, quan abandoneu, encara que sigui puntualment, el lloc de treball (p. ex. amb les tecles Ctrl + Alt + Supr).

Bones pràctiques

A l'hora d'utilitzar el sistema de correu electrònic professional, hem de respectar la legislació vigent i el que s'estableix a les Normes d'ús del correu electrònic establertes per l'empresa. Més enllà d'això, convé tenir presents algunes bones pràctiques per a utilitzar aquesta eina d'una forma respectuosa amb la privacitat de les persones.

Quan volem escriure a més d'un destinatari...

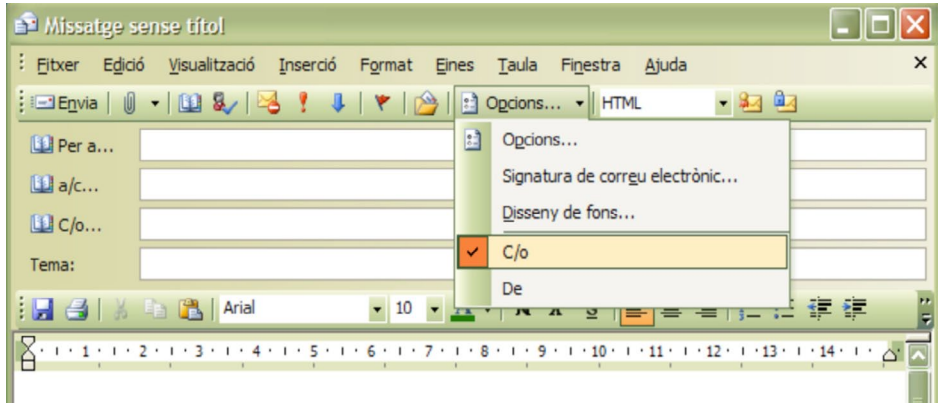
- Abans de contestar un correu que s'ha enviat a diverses persones, cal valorar la necessitat d'enviar la resposta només al remitent o també a la resta.
- L'opció de respondre a tothom farà visible el vostre missatge a totes les persones que hi apareixien com a destinatàries.

I si volem reenviar el correu?

- Utilitzeu l'opció de reenviar només en aquells casos en què tant l'emissor com el contingut del missatge, i tota la informació de la cadena de correus que en formen part, puguin ser accessibles per a la persona destinatària.
- Eviteu la tramesa de missatges piramidals o en cadena, per evitar donar a conèixer indegudament adreces de correu o continguts a terceres persones i per evitar la propagació de virus o programari maliciós *(malware)*.

Què és la còpia oculta (CCO)?

L'opció CCO (còpia de carbó oculta) o C/o (Còpia oculta) permet que, en correus adreçats a una pluralitat de persones destinatàries, les seves adreces o la seva identificació romanguin ocultes per a la resta de persones destinatàries.



Recordeu

Per evitar la divulgació de la resta d'adreces de les persones destinatàries del correu electrònic, utilitzeu l'opció CCO quan no disposeu del seu consentiment o quan no concorri alguna altra circumstància que permeti revelar aquesta dada.

Amb la utilització d'aquesta opció, no només es preserva la confidencialitat de la resta de persones destinatàries sinó que també s'eviten pràctiques de correu brossa *(spam)* o similars.

Cal tenir en compte, però, que en alguns casos el filtre antiinundació *(anti-spam)* pot identificar erròniament aquest tipus de missatges, i classificar-los com a correu brossa.

Es poden adjuntar documents al correu electrònic?

Cal consultar les normes d'ús del correu corporatiu, per conèixer quines són les comunicacions de dades que es poden fer mitjançant el correu electrònic i, si escau, amb fitxers adjunts, qui està autoritzat a realitzar-les, i com s'ha de tractar la informació que es rebi per aquesta via.

Recordeu

Analitzeu, abans d'enviar un fitxer per correu, si conté dades personals. Si és així:

- Assegureu-vos que totes les persones a qui heu adreçat el correu poden accedir a aquesta informació, d'acord amb les seves funcions. Si no fos així, no envieu aquest correu. En cas que fos necessari enviar-lo, seleccioneu la informació que correspongui a cadascuna de les persones destinatàries.
- Utilitzeu tècniques de xifratge de documents, en el cas de les dades que requereixen un nivell alt de seguretat d'acord amb el RLOPD. Recordeu que els correus electrònics i els documents que s'hi adjunten tenen la consideració de suports, a efectes de les mesures de seguretat a aplicar establertes al RLOPD.

Com podem garantir la nostra identitat i l'autenticitat del contingut dels nostres correus electrònics?

Per garantir l'autenticitat i la integritat de les comunicacions, podem emprar la signatura electrònica mitjançant el certificat facilitat per l'empresa, d'acord amb les condicions d'ús que s'estableixin a les normes d'ús del correu electrònic:

☐ Signatura electrònica

Conjunt de dades en forma electrònica que, consignades i/o associades amb d'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.

Es pot generar a partir d'un certificat electrònic.

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

Podeu consultar els passos per **signar electrònicament un correu electrònic** al següent enllaç

Per garantir-ne la confidencialitat, podem emprar el xifratge:

☐ Xifratge

El xifratge transforma el missatge, fent servir una clau, per evitar que qui no la conegui el pugui interpretar. El xifratge garanteix que la informació no sigui intel·ligible ni manipulada per tercers.

La normativa de protecció de dades imposa el xifratge en la transmissió de dades de caràcter personal a través de xarxes públiques o xarxes sense fil de comunicacions electròniques, quan el tractament requereix 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.

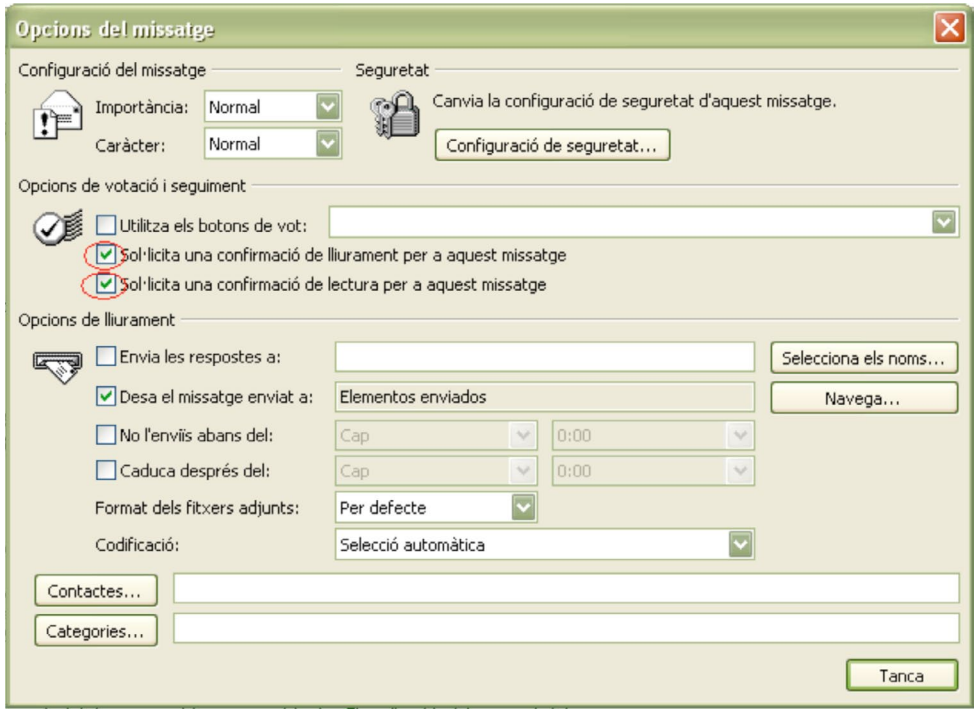
Per desxifrar un missatge, cal tenir instal·lat un programa de xifratge i conèixer la clau que permet desxifrar-lo.

Podeu consultar els passos per **xifrar un correu electrònic** al següent enllaç

Com sabem que s'ha rebut el nostre missatge?

Una errada en la identificació del destinatari o en la transcripció de l'adreça pot comportar que el missatge sigui rebut per una persona diferent a la prevista. En aquest cas, la confidencialitat del contingut del correu electrònic es veu compromesa.

Normalment, els sistemes de correu permeten activar l'opció de confirmació de lliurament o de confirmació de lectura. Aquestes opcions ofereixen més seguretat, atès que permeten conèixer l'èxit de la tramesa. Però cal comprovar, a més, mitjançant la identificació que apareix al missatge de resposta, que el missatge l'ha rebut la persona a la qual anava destinat. Cal tenir en compte, però, que el destinatari pot no autoritzar que s'enviï la confirmació de lliurament o de lectura.



Recordeu

- Comproveu l'adreça del destinatari, abans d'enviar el correu. Si el missatge va adreçat a un grup d'usuaris prèviament configurat, es recomana utilitzar llistes de distribució (si el programa ho permet).
- Utilitzeu, sempre que sigui possible, l'opció de copiar i enganxar en lloc de teclejar les adreces. Així, evitareu les errades que es poden produir en reescriure-les.
- Assegureu que els destinataris són els correctes, quan els seleccioneu del directori corporatiu d'adreces, mitjançant la comprovació d'alguna altra de les informacions que apareix al directori.
- Quan el programa completi automàticament l'adreça que esteu introduint mitjançant el teclat, si l'adreça no us resulta coneguda comproveu-ne la correcció consultant les propietats del contacte.
- Activeu l'opció de confirmació d'entrega i/o confirmació de lectura per part del destinatari, abans d'enviar un missatge, i comproveu que el destinatari previst ha rebut el missatge.
- Podeu incloure, en el peu del missatge, algun text preestablert que recordi la necessitat de destruir el missatge, en cas que hagi estat rebut per error, com també la conveniència de posar-ho en coneixement del remitent. El text podria ser similar al següent:

"AVÍS

Aquest missatge pot contenir informació confidencial i està adreçat únicament al seu destinatari. Si l'heu rebut per error, no el divulgueu a terceres persones, notifiqueu-ho al remitent i esborreu-lo del vostre sistema. Moltes gràcies."

Durant la nostra absència, qui pot contestar els correus?

En supòsits d'absència programada, i amb la finalitat de donar resposta als correus electrònics entrants, es pot activar la funció del missatge de resposta automàtica "Fora d'oficina".

☐ Cal tenir en compte que:

- El missatge d'absència d'oficina permet, a persones que duguin a terme accions d'enviament massiu de correu brossa, validar la vostra adreça com una adreça realment existent.
- Segons quin sigui el contingut del missatge de resposta, potser esteu donant un excés d'informació a la persona que el rebi.
- En donar informació sobre la vostra absència, un tercer pot utilitzar aquesta informació per fer un enviament massiu de correus electrònics a la vostra bústia, amb la finalitat de bloquejar-la.
- En casos d'absència, quan la continuïtat del servei requereixi redireccionar el correu a l'adreça d'un altre treballador, en cas que les normes internes d'ús del correu en permetin un cert ús privat , convé advertir d'aquesta circumstància els vostres contactes personals.

I si volem accedir al correu des de fora de la nostra oficina?

☐ Accés remot

Si l'empresa ho autoritza, l'accés al correu electrònic es podrà fer a través de sistemes remots d'accés, mitjançant dispositius de l'empresa o dispositius personals del treballador o de terceres persones, i també per mitjà de dispositius mòbils, com ordinadors portàtils, telèfons intel·ligents o *smartphones*, tauletes, etc.

Recordeu

Quan per accedir al correu electrònic via web mail s'utilitzin ordinadors d'ús compartit:

- Utilitzeu només protocols segurs, com l'htpps.
- Esborreu el rastre de la vostra navegació.
- Tanqueu la sessió cada vegada que en sortiu.
- No trieu l'opció de recordar la contrasenya que s'ofereix de vegades, per evitar que quedi registrada en aquell ordinador.

☐ Accés per mitjà de dispositius mòbils

Els dispositius mòbils han de comptar amb les mateixes mesures de seguretat que els llocs de treball fixos, però la utilització d'aquest tipus d'accés al correu genera nous riscos que cal prevenir.

Recordeu

- Compliu les polítiques corporatives de seguretat relatives a l'ús d'usuaris i contrasenyes.
- Eviteu l'ús de xarxes Wi-Fi que no ofereixin confiança.
- Instal·leu en aquests dispositius només les aplicacions autoritzades prèviament pel responsable de seguretat o la persona a qui correspongui.
- No emmagatzemeu informació sensible en local en aquests dispositius.
- En cas de robatori o pèrdua, aviseu immediatament el responsable de seguretat de l'empresa o la persona a qui correspongui.
- Alguns dispositius poden configurar-se perquè l'usuari o, si escau, el servidor de correu, puguin bloquejar-los remotament o localitzar-los en cas de pèrdua o robatori.

Correu brossa o *Spam*: Com evitar-lo?

Cal tenir en compte que, les comunicacions publicitàries o promocionals per correu electrònic les han d'haver demanat o autoritzat expressament les persones destinatàries, llevat que es compleixin les condicions següents:

- Hi hagi una relació contractual prèvia, que hi estigui vinculada,
- L'adreça s'hagi obtingut de forma lícita i
- La comunicació es refereixi a productes o serveis de la mateixa empresa, similars als que havien estat contractats.

Recordeu

- Eviteu respondre correus identificats com a correu brossa *(spam)* o de procedència dubtosa. Això validaria l'adreça de correu com a existent i probablement generaria l'enviament de més correu brossa.
- No cliqueu sobre els anuncis que apareguin als missatges de correu susceptibles de ser *spam*.
- No obriu fitxers adjunts de missatges amb emissors desconeguts, sense haver-los analitzat abans amb un programa antivirus.
- No activeu l'opció de vista prèvia.
- Vigileu a qui faciliteu l'adreça de correu electrònic.
- Eviteu participar en els correus electrònics en cadena.
- Envieu missatges amb còpia oculta.
- Esborreu les adreces del missatge anterior quan reenvieu un correu electrònic.
- No publiqueu l'adreça de correu electrònic a cercadors, fòrums, adreces de contacte o pàgines web, llevat que sigui estrictament necessari.
- Instal·leu filtres automàtics antiinundació o *anti-spam* o de control del correu no desitjat.
- Utilitzeu programes antivirus i que detectin programari maliciós *(malware)*.
- Llegiu atentament les polítiques de privacitat i les condicions de cancel·lació quan, en exercici de les vostres funcions, contracteu un producte o servei o feu una subscripció en línia.

Altres mesures de seguretat...

Recordeu

- Adapteu les opcions de seguretat del vostre correu a la naturalesa de les dades que preveieu rebre o comunicar.
- Situeu i orienteu 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 vostre lloc de treball.
- No instal·leu programari no autoritzat per l'empresa.
- Programeu l'eliminació, de forma immediata, dels missatges que puguin contenir virus o *malware*. L'esborrat complet requereix eliminar-los, també, de la paperera de reciclatge.
- Comuniqueu a l'àrea encarregada de la seguretat de la informació qualsevol incidència que es detecti en el sistema, d'acord amb el protocol que estableixi l'empresa.