

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI26-01
	ÚS DEL CORREU ELECTRÒNIC	
	N. versió: 1.0	Pàg. 1 / 9



**Llicència Creative Commons:**

**Reconeixement – No Comercial – Compartir Igual 2.5.**


**Sou lliure de copiar, distribuir i comunicar públicament l'obra, així com de fer-ne obres derivades, en les següents condicions:**



**Reconeixement.** Heu de reconèixer els crèdits de l'obra de la manera especificada per l'autor o el licenciadador.



**No comercial.** No podeu utilitzar aquesta obra per a finalitats comercials.



**Compartir amb la mateixa llicència.** Si altereu o transformeu aquesta obra, o en genereu obres derivades, només podeu distribuir l'obra generada amb una llicència idèntica a aquesta.


- Quan reutilitzeu o distribuïu l'obra, heu de deixar ben clar els termes de la llicència de l'obra.
- Algunes d'aquestes condicions pot no aplicar-se si obteniu el permís del titular dels drets d'autor.

**Podeu trobar el text legal de la llicència a:** [Creative Commons Attribution-NonCommercial-ShareAlike 2.5 License](https://creativecommons.org/licenses/by-nc-sa/2.5/)

## ÍNDEX

RESUM .....	2
1. OBJECTIU I MOTIVACIÓ .....	3
2. ÀMBIT I VIGÈNCIA .....	3
3. COMPLIMENT AMB ELS REQUISITS LEGALS I ESTÀNDARDS DE SEGURETAT .....	3
4. DESCRIPCIÓ .....	3
Norma .....	3
Recomanacions .....	6
5. CONTROL .....	7
6. PENALITZACIONS .....	7
7. DIVULGACIÓ .....	7
8. REVISIÓ .....	7
9. GLOSSARI DE TERMES .....	7
10. DOCUMENTACIÓ REFERENCIADA .....	8
11. PARAULES CLAU .....	8
12. HISTÒRIC DEL DOCUMENT .....	8

Versió	Redactat / revisat per	Aprovat per	Data aprovació	Data publicació
1.0.	CTTI- Qualitat i Seguretat	Comitè de Direcció del CTTI		

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI26-01
	ÚS DEL CORREU ELECTRÒNIC	
	N. versió: 1.0	Pàg. 2 / 9

## RESUM

**1. Objectiu:** Definir un conjunt de mesures i millors pràctiques que determinen un bon ús del correu electrònic, per tal de protegir la informació, complir amb la legislació vigent i garantir un bon funcionament dels sistemes.


**2. Àmbit:** Usuaris de correu electrònic sota domini tutelat o titularitat de la Generalitat de Catalunya.

### 3. Descripció:

- Bon ús del correu (finalitat de la utilització, comportament ètic, inclusió d'un peu de correu, ...).
- Sol·licitud de bústies de correu.
- Comunicació d'incidències.
- Protecció de la informació (necessitat de protegir informació confidencial o privada, ús de certificat digital, reenviament automàtic, peu de correu, ...).
- Accés a bústies de correu i llistes de distribució (ús correcte de la contrasenya d'accés, no utilitzar el recordatori de contrasenya, creació de llistes de distribució, ...).
- Programari de correu electrònic autoritzat.
- Retenció de correu electrònic.
- Suport en l'ús del correu electrònic

### 4. Recomanacions:

- Sobre el contingut del missatge.
- Sobre l'enviament dels missatges.
- En cas d'absència de l'oficina.

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI26-01
	ÚS DEL CORREU ELECTRÒNIC	
	N. versió: 1.0	Pàg. 3 / 9

## 1. OBJECTIU I MOTIVACIÓ

Definir les mesures que determinen un bon ús del correu electrònic, així com algunes recomanacions, per tal de:

- Protegir la informació i la imatge de la Generalitat de Catalunya.
- Assegurar el compliment de la legislació vigent, especialment en matèria de serveis de la societat de la informació, protecció de dades i comunicacions electròniques.
- Garantir el correcte funcionament dels sistemes de correu electrònic.
- Donar a conèixer als usuaris els principals riscos i conceptes de privacitat i seguretat relacionats amb el correu electrònic.

L'ús generalitzat del correu electrònic a la Generalitat de Catalunya en el desenvolupament diari de la seva tasca, fa imprescindible que els usuaris siguin conscients de la seva responsabilitat en l'ús d'aquest sistema de comunicació i en la protecció de la informació accessible a través d'aquest mitjà.

Cal considerar que tot correu electrònic emès sota **domini** tutelat o titularitat de la Generalitat de Catalunya podria ser considerat pel receptor com un comunicat oficial i per tant caldrà tenir màxima cura en els continguts dels missatges. No obstant això, el fet de disposar d'un compte de correu electrònic sota **domini** tutelat o titularitat de la Generalitat no autoritza l'emissor a representar la Generalitat de Catalunya o a actuar en el seu nom més enllà de la seva habilitació específica o per raó del seu càrrec.

## 2. ÀMBIT I VIGÈNCIA

Aquesta guia afecta a tots els usuaris de correu electrònic sota **domini** tutelat o titularitat de la Generalitat de Catalunya, tant si és personal intern com si es tracta de personal extern en prestació de serveis *[Cada organització pot especificar els dominis utilitzats]*.

Entrarà en vigor el dia **1 de Juny de 2006**.

Aquesta guia romandrà vigent fins la propera versió aprovada de la mateixa.

## 3. COMPLIMENT AMB ELS REQUISITS LEGALS I ESTÀNDARDS DE SEGURETAT

La present guia proporciona cobertura als següents controls de la ISO 17799:2005:

- 10.4.1 Controls contra codi maliciós
- 10.8.1 Polítiques i procediments per l'intercanvi d'informació
- 10.8.4 Missatgeria electrònica
- 10.10.1 Registres d'auditoria (logging)
- 11.3.1 Ús de les contrasenyes
- 11.4.2 Autenticació d'usuari per les connexions externes
- 11.5.1 Processos de connexió segurs
- 11.5.2 Identificació i autenticació d'usuaris
- 12.2.3 Integritat dels missatges
- 13.1.1 Notificar dels esdeveniments de seguretat
- 15.1.2 Drets de la propietat intel·lectual


## 4. DESCRIPCIÓ

### Norma

#### Bon ús del correu

N1. L'ús del correu de la Generalitat s'ha de limitar a l'àmbit professional, és a dir que només es farà servir pel compliment de les tasques i funcions assignades. Si excepcionalment es vol fer servir el correu electrònic per propòsits personals, caldrà fer servir un compte de correu webmail (accés a través de navegador) sota **domini** diferent del tutelat o titularitat de la Generalitat de Catalunya, i sempre complint amb aquesta política. No es podran configurar comptes personals en el programari de correu estàndard.

N2. El correu electrònic no pot ser utilitzat per crear o enviar missatges amb contingut ofensiu, poc ètic, amenaçador, de calúmnia o que pugui suposar minva en la imatge i consideració de la Generalitat de Catalunya. La Generalitat no es fa responsable del contingut dels missatges en cas d'accions penals o civils contra l'emissor del/s missatge/s emès/os.

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI26-01
	ÚS DEL CORREU ELECTRÒNIC	
	N. versió: 1.0	Pàg. 4 / 9

Si alguna persona al servei de la Generalitat de Catalunya rep un correu amb continguts d'aquest tipus de qualsevol usuari de correu de la Generalitat de Catalunya, haurà de posar-ho en coneixement del seu propi superior.

- N3. Es prohibeix utilitzar el correu per la difusió interna o externa de correu no desitjat (*spam*), sigui o no massiva, de virus i altre codi maliciós, així com per l'enviament de *cartes en cadena* o *cartes bomba*.
- N4. Es prohibeix la tramesa d'un mateix missatge simultàniament a un gran nombre de bústies electròniques, llevat que estigui justificada en el compliment de les tasques encomanades. *[Cada organització haurà d'establir quan s'escaigui les pautes per enviament massiu de missatges per part de caps de comunicació o premsa, que s'haurà de basar en llistes de distribució o programari específic de correu, i mai en l'enviament des del client de correu a un número elevat d'adreces de correu electrònic]*.
- N5. Quan es reenvia un missatge, no es pot manipular el contingut de la informació del missatge original, si no s'adverteix al receptor del tipus de tractament / alteració que se n'ha fet.
- N6. Cal incorporar un comiat i una signatura al peu del correu amb informació suficient per a què el destinatari conegui en tot moment qui és l'emissor del missatge dins de la Generalitat de Catalunya i quines són les seves dades de contacte. Això cobra especial importància en el cas que el missatge sigui reenviat.

Es presenta a continuació una proposta de signatura de correu *[Cada organització especificarà la seva]*:

#### Nom de la persona

Unitat funcional / Àrea funcional / o càrrec

Generalitat de Catalunya

Nom de l'organització

Carrer, número, pis

Codi postal Població

Tel. 9xxxxxxx

Fax. 9xxxxxxx

[xxxx.xxxx@gencat.net](mailto:xxxx.xxxx@gencat.net) (o domini Generalitat pertinent)

#### Sol·licitud de bústies de correu

- N7. Per sol·licitar una bústia de correu, el procediment a seguir és el següent: *[Cada organització haurà de descriure o fer referència al procediment establert]*.


En cas de fer servir el correu corporatiu, consultar la intranet del CTTI ([Àrea Pública / Quins serveis Oferim? / Serveis TIC Centrals Continuats / Catàleg de Serveis / Comunicacions Electròniques / Correu](#)).

#### Comunicació d'incidències

- N8. Qualsevol incidència (problema o mal funcionament) o anomalia (comportament estrany o inesperat) del correu s'haurà de notificar el més aviat possible mitjançant el procediment habitual *[Cada organització farà referència al seu procediment de notificació d'incidències. En cas de tractar-se de correu corporatiu, caldrà seguir el procediment especificat a la intranet del CTTI]*.
- N9. Els servidors de correu estan dotats de programari antivirus i detectors d'altre codi maliciós, que escanegen els missatges d'entrada i sortida per prevenir possibles infeccions. *[Cada organització haurà d'especificar quin tractament dona als missatges infectats d'entrada o sortida]*. No obstant, si es té sospita d'infecció per virus o altre codi maliciós, no fer servir el correu per evitar-ne la propagació.

#### Protecció de la informació

- N10. Per enviar informació confidencial a través del correu electrònic, caldrà utilitzar mitjans de seguretat addicional, doncs el correu en sí mateix no és un mitjà de comunicació segur. Quan es disposi de certificat digital, i es tingui la certesa que el receptor podrà desxifrar el missatge, es recomana fer-lo servir. En cas de no disposar de certificat digital es poden xifrar els fitxers que contenen la informació utilitzant, per exemple, les opcions de xifrat amb contrasenya que inclouen les opcions de gravació de fitxers amb seguretat d'alguns programes ofimàtics (en aquest cas, cal triar les opcions de clau més llarga, com a mínim de 128 bits i posar una paraula de pas de com a mínim 8 posicions, combinant

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI26-01
	ÚS DEL CORREU ELECTRÒNIC	
	N. versió: 1.0	Pàg. 5 / 9

lletres, números i símbols, majúscules i minúscules) o programari de xifrat específic (cada organització indicarà si és possible accedir a aquest programari i quin és el circuit).

Si el missatge conté dades de caràcter personal de **nivell alt**, l'encriptació de la informació és indispensable per donar compliment a la LOPD (Llei orgànica de protecció de dades de caràcter personal).

N11. Caldrà utilitzar un **certificat digital** reconegut quan sigui necessari garantir jurídicament la identitat de l'emissor, la integritat de la informació continguda, la confidencialitat d'aquesta informació i la no refutació per part del receptor. *[Cada organització haurà d'indicar quines són les CA autoritzades, qui pot demanar certificat i quin és el procediment de sol·licitud / aprovació de certificat digital o fer referència a un procediment específic de certificats digitals].*

N12. Està prohibit activar les opcions de reenviament automàtic de correu cap a l'exterior sense autorització d'un superior, per tal d'assegurar un bon control de la informació que surt de l'àmbit de la Generalitat.

N13. L'accés al correu des de l'exterior s'ha de fer de forma segura. En el cas de correu corporatiu, per accedir al correu des de fora de la xarxa habitual, la Generalitat de Catalunya posa a disposició dels treballadors l'accés per internet mitjançant web-mail (correu.gencat.net o pim.gencat.net) segons el tipus de correu. En cas de dubte, consultar ...*[Cada organització haurà d'indicar quin és el punt de contacte. Si l'organització disposa d'altres opcions de connexió segura com VPN per exemple, caldrà especificar-les en aquest punt].*

N14. Cal posar una clàusula de forma estàndard al peu del correu per protegir la possible confidencialitat de la informació continguda al missatge. Si el sistema no afegeix aquesta clàusula automàticament, cal configurar la bústia de correu per tal que ho faci en l'enviament i reenviament de missatges, Una proposta de clàusula a afegir és la següent:

\*\*\*\*\*

La informació continguda en aquest missatge és confidencial. Si vostè no és un dels destinataris definits o algú responsable de fer-los-el arribar, aleshores ha rebut aquest missatge per error i no està autoritzat a llegir-lo, retenir-lo o distribuir-lo. Li preguem que esborri el missatge i els documents annexats, ho comuniqui immediatament al remitent i s'abstingui d'utilitzar les dades personals que hi consten.

La información contenida en este mensaje es confidencial. Si Usted no es uno de los destinatarios definidos o alguien responsable de hacérselo llegar, ha recibido este mensaje por error y no está autorizado a leerlo, retenerlo o distribuirlo. Le rogamos borre el mensaje y documentos anexos, lo comunique inmediatamente al remitente y se abstenga de utilizar los datos personales que figuran en el mensaje.

\*\*\*\*\*

N15. No escriure en un correu electrònic totes les dades d'accés a un sistema o document (identificador d'usuari, contrasenya, clau de desenciptació, ...), independentment de qui les estigui demanant. Des de la Generalitat no s'utilitzarà el correu electrònic per demanar aquest tipus d'informació.

#### Accés a bústies de correu i **lístes de distribució**


N16. L'accés a les bústies de correu personals es concedeix individualment i es realitza a través d'un mitjà d'autenticació segur (identificador i contrasenya, certificat digital, ...).

N17. És responsabilitat dels usuaris garantir un ús adequat de les seves credencials d'accés (identificador i contrasenya / certificat / etc.).

N18. En cas que de forma temporal o permanent sigui necessari que altres persones accedeixin a la bústia de l'usuari, ja sigui només per lectura, o per llegir i enviar missatges en el seu nom, mai no es farà donant-los a conèixer les credencials d'accés de l'usuari, sinó que l'usuari haurà de fer-ho a través de les opcions de "Delegació d'accés", quan el programari de correu ho permeti. De no ser possible, una altra opció per permetre la lectura és reenviar el correu cap a la bústia de l'altra persona, quan aquesta bústia sigui interna de la Generalitat.

N19. *[Quan l'accés es faci a través d'identificador i contrasenya, el sistema obligarà a canviar la contrasenya el primer cop que s'hi accedeixi].* És responsabilitat de l'usuari complir la **Norma de contrasenyes**, especialment en els aspectes de confidencialitat i seguretat de la paraula de pas.

N20. Per raons de seguretat, està prohibit activar les opcions de "Recordatori de contrasenya" per accedir a les bústies, encara que això comporti la necessitat d'autenticar-se cada vegada que s'activa l'enviament i recepció de missatges.

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI26-01
	ÚS DEL CORREU ELECTRÒNIC	
	N. versió: 1.0	Pàg. 6 / 9

N21. En el cas de dispositius mòbils a través dels quals sigui possible accedir al correu electrònic, cal activar una contrasenya d'accés al dispositiu, per protegir la informació que hi resideix o a la qual s'hi pot accedir.

N22. Les *l·listes de distribució* s'utilitzen per difondre de manera massiva avisos, alarmes i comunicats. *[Cada organització ha de definir qui té autorització per crear una llista de distribució global (aquella que l'usuari no pot crear localment, sinó que ha de ser creada per un administrador)].* En el moment de crear-la cal definir qui tindrà accés a aquesta *llista de distribució* i qui serà el responsable del seu manteniment.

#### Programari de correu electrònic autoritzat

N23. Només es podrà utilitzar programari de correu electrònic autoritzat per l'òrgan o unitat que té atribuïda la competència *[Cada organització haurà d'especificar qui té aquesta competència i quin és l'estàndard tecnològic].*

#### Retenció del correu electrònic

N24. Com a norma general, tret que s'hagi fet servir una signatura electrònica, el correu electrònic no es pot considerar com un registre de negoci formal, al no garantir l'autenticitat, integritat, exactitud, completesa, no refutació i preservació de l'evidència. És a més informació subjecta a canvis de versió o programari, de manera que no s'hauria de guardar com a registre permanent. Existeixen altres maneres per formalitzar decisions, compromisos, ... com actes de reunions, documents firmats, registres autoritzats de veu, etc.

N25. Cal ser selectiu a l'hora d'emmagatzemar correus, i guardar només aquells que puguin ser útils en el desenvolupament de la feina.

N26. No guardar els missatges de manera sistemàtica i permanent, i fer revisions de depuració periòdica.

N27. Guardar els missatges que s'hagin de conservar, en format no xifrat, en una ubicació que tingui garanties de confidencialitat, integritat i continuïtat. *[Cada organització haurà d'indicar quina és la política aplicada – si hi ha un 'espai de memòria individual, si es realitzen còpies de seguretat periòdiques, capacitat màxima de les bústies, procediments de depuració automàtica periòdica, ... En cas que s'emmagatzemi el contingut dels correus electrònics, caldrà fer-ho constar indicant la finalitat per la qual això es fa].*

#### Suport en l'ús del correu electrònic

N28. Per qualsevol dubte sobre el funcionament del correu, el redactat d'aquesta política o la manera de posar en pràctica alguna de les normes / recomanacions incloses en aquest document, cal adreçar-se a *[Cada organització especificarà les dades de contacte].*

### **Recomanacions**

#### Sobre el contingut del missatge

R1. El correu electrònic no sempre substitueix el telèfon i no garanteix la lectura per part del receptor. Abans d'enviar un missatge cal considerar si és el mitjà més adient per fer-ho. En cas d'urgència, és convenient advertir al receptor per telèfon de què se li ha enviat un missatge i de què s'agraïria una ràpida resposta.


R2. Escriure els missatges amb llenguatge professional; no ser massa informal o col·loquial. No escriure res que no es posaria en una carta. Cal ser neutral i evitar llenguatge sexista, insultant, abusiu o discriminador, que pogués ofendre o irritar als altres.

R3. Sempre que sigui possible, incorporar la informació al propi missatge i no adjuntar documents.

R4. En el "Tema", escriure una frase que ajudi al receptor a saber de què tracta el missatge, i li permeti filtrar-lo, prioritzar-lo, arxivar-lo i més endavant recuperar-lo.

R5. No obrir missatges de correu ni documentació adjunta si el remitent és totalment desconegut, l'adreça de correu és totalment desconeguda, el títol del missatge no proporciona una descripció del possible contingut del missatge, o es tracta d'un missatge estrany que no s'esperava, independentment de qui sigui l'emissor. Possiblement es tracta de *spam* o són missatges generats per virus o altre codi maliciós. Esborrar aquests missatges sense obrir-los i, a continuació, eliminar-los de la paperera.

R6. Per evitar la sobrecàrrega de la xarxa, no adjuntar imatges o fitxers de gran volum al missatge (fitxers amb imatges, fotos, presentacions, ...) si existeix una altra manera de compartir la informació amb el destinatari (directoris compartits, espais de col·laboració, ...). *[Si hi ha alguna regla de retenció de*

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI26-01
	ÚS DEL CORREU ELECTRÒNIC	
	N. versió: 1.0	Pàg. 7 / 9

*correu de gran volum per enviament en moments de baixa ocupació de la xarxa, o de màxima capacitat d'enviament, cal especificar-ho en aquest punt].*

#### Sobre l'enviament de missatges

- R7. Cal ser respectuós amb el temps dels altres. Enviar missatges de correu únicament a aquelles persones amb una necessitat legítima de la informació. No respondre a missatges si no aporten valor afegit.
- R8. Abans d'enviar un missatge a una llista de distribució cal analitzar si no existeixen altres eines de comunicació massiva (butlletins, intranets, ...). Cal analitzar si realment tots els membres de la llista estan interessats en aquell missatge.
- R9. Dirigir el missatge (camp "Per a:") a les persones de les que s'espera un acció o resposta. Enviar còpies (camp "a/c") a les persones que es vol mantenir informades, però de les que no s'espera cap acció o resposta.
- R10. Si es contesta un missatge, incorporar el cos del missatge al que es respon, per mantenir intacta la cadena d'informació.
- R11. Abans de reenviar un missatge, cal assegurar-se que tota la informació que s'està reenviant pot ser desvetllada al destinatari.
- R12. Configurar els missatges amb l'opció "Importància Alta" només en els casos realment urgents.
- R13. Utilitzar les opcions de seguiment dels missatges enviats (acusament de recepció, ...) quan realment sigui necessari, i tenint en compte que només funcionarà si el servidor de correu del receptor està configurat per fer-ho.
- R14. No contestar mai missatges de *spam*, ni respondre a l'opció de "donar de baixa la subscripció" d'aquests missatges, per evitar donar a conèixer als emissors de *spam* que es tracta d'una adreça de correu vàlida, i evitar així que pugin intensificar l'enviament de correu brossa. *[En cas que el filtre antispam ubiqüi els missatges d'spam en una carpeta del client diferent de la d'entrada, caldrà especificar-ho en aquest punt, així com explicar què s'espera que l'usuari faci amb aquests missatges].*

#### En cas d'absència de l'oficina

- R15. En cas d'absència per més d'un dia, quan el programari de correu ho permeti, cal utilitzar l'opció "fora de l'oficina", indicant el primer i últim dia d'absència, per notificar a les persones que ens envien missatges fins quan estarem absents i amb qui poden contactar en cas d'urgència. ▴

### 5. CONTROL

Per raons de seguretat, per garantir el bon funcionament dels sistemes de correu electrònic, la Generalitat es reserva el dret de monitorar l'origen i el destí dels missatges de correu electrònic i el volum de correu electrònic enviat i rebut. Mai no s'accedirà i/o revelarà al contingut dels missatges, llevat que sigui per motius de seguretat fonamentats o requeriment legal, havent de donar compliment en aquests casos als procediments legals establerts.

### 6. PENALITZACIONS

L'incompliment de la norma pot comportar l'adopció de mesures de restricció o de suspensió de l'ús del correu electrònic i pot determinar, si s'escau, l'aplicació del règim disciplinari corresponent.

En cas d'incompliment d'aquesta guia per part de personal subcontractat, aplicaran les penalitzacions recollides en el contracte de la prestació del servei.

### 7. DIVULGACIÓ

El CTTI publicarà aquesta guia a la seva intranet.


### 8. REVISIÓ

Aquesta guia es revisarà anualment.

### 9. GLOSSARI DE TERMES

Cartes bomba: Missatges que es reenvien repetidament a un o diversos receptors, per interferir / perjudicar al receptor en l'ús del seu correu electrònic.



 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI26-01
	ÚS DEL CORREU ELECTRÒNIC	
	N. versió: 1.0	Pàg. 8 / 9

**Cartes en cadena:** Missatges que conviden a reenviar el mateix missatge a un determinat número de persones. Típicament prometen bona sort, fortuna, i el seu objecte sovint és el de recol·lectar adreces.

**Certificat digital:** El certificat digital és un sistema d'acreditació que permet a les parts tenir confiança en les transaccions a Internet, doncs garanteix la identitat del seu posseïdor a Internet mitjançant un sistema segur de claus administrat per una tercera part de confiança, l'autoritat de certificació. El certificat permet realitzar un conjunt d'accions de forma segura i amb validesa legal, que varia segons el tipus de certificat: signar documents, xifrar missatges, entrar a llocs restringits, identificar-se davant l'Administració, etc.

**Dades personals de nivell alt:** Dades d'una persona física referents a la seva ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual i aquelles dades recollides amb una finalitat policial sense consentiment de la persona afectada.

**Dades personals de nivell mig:** Dades d'una persona física referents a serveis financers contractats, solvència patrimonial i crèdit, infraccions administratives o penals, hisenda pública, i informació que permeti avaluar la personalitat de la persona.

**Domini:** Nom amb què una empresa o organització es dona a conèixer a Internet, i que figura a la dreta de la @ en una adreça de correu electrònic. Alguns dels dominis tutelats o titularitat de la Generalitat de Catalunya són: *gencat.net*, *agaur.gencat.net*, *aqucatalunya.org*, *audiovisualcat.net*, *bnc.es*, *cema-sa.org*, *cidem.gencat.net*, *diasensecotxes.org*, *icaen.gencat.net*, *icfinances.com*, *iemed.org*, *meteocat.com*, *meteocatserveis.com*, *mnac.es*, *parlamente-cat.es*, *parlament-cat.net*, *presidencia.gencat.es*, *tdtcat.net*, *xij.gencat.net*.

**Llista de distribució:** És un conjunt d'adreces de correu electrònic que s'agrupen sota una única adreça de correu electrònic. Quan es fa un enviament a una llista de distribució, s'està fent l'enviament a totes les adreces incloses a la llista. La creació de llistes facilita l'enviament de missatges a grups de persones a qui ens adrecem habitualment de forma conjunta, doncs evita haver d'escriure les seves adreces de correu electrònic cada vegada una a una i en pot garantir la privacitat.

Generalment els clients de correu permeten la creació de llistes de distribució personals, accessibles únicament per l'usuari que les ha creat [*Consultar "Instruccions per la creació de llistes de distribució personals"*].

Les llistes de distribució globals, visibles per qualsevol usuari del sistema de correu, han de ser creades per l'administrador del sistema.

**Spam:** És la pràctica d'enviar missatges de correu electrònic no sol·licitats. Generalment es tracta de publicitat de productes, serveis o pàgines web, però es pot considerar spam l'emissió d'un correu electrònic no sol·licitat. Les adreces de correu electrònic acostumen a ser robades, comprades, recol·lectades per la web o preses de *cartes en cadena*.

## 10. DOCUMENTACIÓ REFERENCIADA

- GE-GUI19 Guia de contrasenyes.
- GE-PRO01 Procediment de notificació d'incidents de seguretat.
- Procediments sobre correu corporatiu de la Generalitat: consultar la intranet del CTTI ([Àrea Pública / Quins serveis Oferim? / Serveis TIC Centrals Continuats / Catàleg de Serveis / Comunicacions Electròniques / Correu](#)).

## 11. PARAULES CLAU

Correu electrònic, bústia de correu, Exchange, iPlanet, Outlook, Lotus Notes, política, usuari.

## 12. HISTÒRIC DEL DOCUMENT

Modificacions que incorpora cada versió.

### Versió 1.0


Redacció inicial del document

Dates d'inici de cada fase:

<i>Detecció de necessitat</i>	<i>Fase de Treball</i>	<i>Fase de discussió</i>	<i>Fase d'aprovació</i>	<i>Fase de difusió</i>	<i>Fase de suport</i>
6/2005	7/2005	2/2006	10/10/2006	13/10/2006	1/1/2007

Equip de treball: Qualitat i Seguretat: Silvia Garre, Josep Mangas, Oficina Seguretat (Indra)



 Generalitat de Catalunya <b>Centre de Telecomunicacions i Tecnologies de la Informació</b>	<b>GUIA</b>	GE-GUI26-01
	<b>ÚS DEL CORREU ELECTRÒNIC</b>	
	N. versió: 1.0	Pàg. 9 / 9

Equip de treball: Qualitat i Seguretat: Silvia Garre, Josep Mangas, Oficina Seguretat (Indra)

Equip de discussió:

1a revisió (juny 2005): AE (Jl. Grau, A.Inarejos) IiT (X.Milà, J.Pérez, A.Haro, A.Massó, Ll.Coma i alguns gestors tecnològics, T.Escuín, F.Parés), AC (J.Gabaldà, P.Solà, I.Laquente), CiE (Ll.Olivé), AProv (A.Rami), AJ (G.Domènech, JM.Prats), Com (E.Roure), QiS (T.Roy), Funció Pública (Maite Jiménez, Josep Lluís Rodríguez, Josep Purgimon), ACA (Jaume Oliva, Joan Francesc Peracaula).

2a revisió (setembre 2006):CTTI – Innovació i Tecnologia: Emili Platel (+ equip architectures), Joan Pérez (+ equip enginyeria).

Comentaris rebuts: Ll.Coma (+ gestors tecnològics), F.Parés, A.Massó, T.Escuín, I.Laquente, A.Rami, JM.Prats i JF.Peracaula.

Òrgan aprovador: Comitè de Direcció del CTTI

Equip de suport: Oficina Seguretat