ÍNDEX



| Versió | Redactat / revisat per | Aprovat per | Data aprovació | Data publicació |
|---|---|---|---|---|
| 1.0 | CTTI – Qualitat i Seguretat | Comitè de Direcció del CTTI | 26/05/2006 | 01/06/2006 |
| | | | | |
| | | | | |
| | | | | |

**RESPONSABLE DEL DOCUMENT**: Josep Mangas (CTTI – Qualitat i Seguretat)

## RESUM

### OBJECTIU

Definir els controls de seguretat que cal aplicar al correu electrònic, amb l'objectiu de garantir la confidencialitat, integritat i disponibilitat dels missatges i del servei.

### ÀMBIT

Sistemes de correu electrònic de la Generalitat de Catalunya.

## 1 OBJECTIU

Definir els controls de seguretat que cal aplicar al correu electrònic de la Generalitat de Catalunya, per tal de cobrir les necessitats dels usuaris, garantir la integritat i confidencialitat / privacitat dels missatges i la disponibilitat del servei.

Aquesta guia presenta el conjunt de controls o contramesures a aplicar als sistemes de correu, avaluats en termes de confidencialitat, integritat i disponibilitat, per tal de combatre potencials amenaces i atacs al servei, i a la informació que a través d'aquest s'intercanvia.

## 2 ÀMBIT I VIGÈNCIA

Aquesta guia va destinada als responsables i administradors de sistemes de correu electrònic sota domini tutelat o titularitat de la Generalitat de Catalunya, per tal que aquests, basant-se en una anàlisi dels potencials riscos de seguretat, puguin triar els controls més adients a les particularitats de l'organització a la que s'està donant servei.

No és objectiu d'aquesta guia de servei establir les solucions tecnològiques per la implantació de cada tipus de control.

En els casos que l'explotació del servei estigui externalitzada, caldrà exigir l'aplicació dels controls de seguretat a nivell contractual.

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 a aspectes recollits en els següents controls de la ISO 17799:2005:

- 6.2.3 Requeriments de seguretat en els acords amb les terceres parts
- 10.4.1 Controls contra codi maliciós
- 10.10.1 Registres d'auditoria (logging)
- 11.4.4 Protecció dels ports de configuració i diagnòstic remot
- 11.5.1 Processos de connexió segurs
- 11.5.3 Sistema de gestió de les contrasenyes
- 11.6.1 Restricció d'accés a la informació
- 13.1.1 Notificar dels esdeveniments de seguretat

## 4 DESCRIPCIÓ DELS CONTROLS

Es presenten a continuació els possibles controls de seguretat per un sistema de correu electrònic, orientats a garantir la confidencialitat, privacitat integritat i disponibilitat del servei, així com el compliment de la legislació vigent. Aquests s'agrupen per grups d'accions o procediments operatius orientats a combatre les amenaces a les quals el servei de correu electrònic està exposat. Sota la columna "categoria", s'especifiquen els aspectes de seguretat que cada control reforça (confidencialitat – C, integritat – I, disponibilitat – D).

### *4.1. MN – Monitoratge*

| **OBJECTIUS** | |
|---|---|
| Monitorar el servei de correu electrònic (no el contingut dels missatges): registre d'intents d'accés al servei de correu electrònic, cavis de configuració, origen i destí dels correus, ... per tal de poder conduir futures investigacions en cas de necessitats i atribuir-ne responsabilitats. | |
| **CARACTERÍSTIQUES** | |
| **Descripció** | **Categoria** |
| C1. Registre d'intents d'accés al correu amb èxit o fallits, i registre d'incidents de correu en general. | C D |
| C2. Registre de tasques administratives o de seguretat. Si el sistema ho suporta, caldrà registrar també qualsevol canvi o resultat. | C D |

| | |
|---|---|
| C3. Registre de caigudes del servei. | C D |
| C4. Eines per rastrejar l'accés dels administradors del sistema. | C D |
| C5. Eines per rastrejar canvis de configuració del servei. | C I D |
| C6. Caldrà consensuar amb el CTTI si és necessari registrar l'accés a arxius o objectes i a impressores. | C I D |

### *4.2. ID – Intercanvi de dades*

Aquests controls pretenen assegurar la confidencialitat, integritat i disponibilitat dels canals de transmissió de dades, és a dir, que pretenen establir la seguretat en les comunicacions.

#### *4.2.1. ID.C – Confidencialitat en l'intercanvi de dades*

| **OBJECTIUS** | |
|---|---|
| Prevenir l'accés no autoritzat als missatges de correu electrònic durant la seva transmissió i la seva possible manipulació | |
| **CARACTERÍSTIQUES** | |
| **Descripció** | **Categoria** |
| C7. Quan la criticitat de les dades ho requereixi, encriptació de les dades en trànsit, que es pot fer a tres possibles nivells: fitxers continguts als missatge, missatge complert o canal segur. | C I |
| C8. Configurar el servei de correu, quan sigui possible, per a què incorpori automàticament al peu dels correus emesos i reenviats una clàusula de confidencialitat. Aquesta incorporació no serà possible si el servei no és capaç de detectar si un correu ha estat signat electrònicament en origen, ja que sinó no es mantindria la integritat de la signatura, degut a què es modificaria el contingut del correu després de la signatura del mateix.<br>Proposta de clàusula:<br>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 qualsevol document adjunt que pogués contenir, ho comuniqui immediatament al remitent i s'abstingui d'utilitzar les dades personals que hi consten.<br><br>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 que borre el mensaje y cualquier documento adjunto que pudiera contener, lo comunique inmediatamente al remitente y se abstenga de utilizar los datos personales que figuran en el mensaje.<br>********** | C |
| C9. Configuració del servidor de correu per què elimini per defecte l'enviament de qualsevol informació relativa a la versió del programari del servidor de correu i del sistema operatiu sobre el qual funciona. | C D |

#### *4.2.2. ID.I – Integritat en l'intercanvi de dades*

| **OBJECTIUS** | |
|---|---|
| Prevenir l'alteració, cancel·lació o substitució no autoritzada dels missatges en trànsit, i el no repudi per part del receptor del missatge. | |
| **CARACTERÍSTIQUES** | |
| **Descripció** | **Categoria** |
| C10. Per garantir la traçabilitat del recorregut del missatge, activació de controls d'autenticació del missatges rebuts, que permetin garantir que hi ha coincidència | I |

| | |
|---|---|
| entre el domini de l'emissor i del servidor des del qual ha estat enviat, i que rebutgin qualsevol missatge que no superi aquest control. | |
| C11. Possibilitar l'ús de la signatura digital. | C I D |

### *4.3. FI – Fiabilitat de les dades*

| **OBJECTIUS** | |
|---|---|
| Monitorar el tràfic il·legal per tal de detectar i restaurar la integritat del programari i les dades. El servei de correu ha de garantir la integritat dels correus que hi resideixen. | |
| **CARACTERÍSTIQUES** | |
| **Descripció** | **Categoria** |
| C12. Configurar el servidor de correu i instal·lar software antivirus per verificar tots els missatges d'entrada i sortida, incloent la documentació adjunta. L'antivirus haurà de ser capaç de detectar l'existència de virus en fitxers comprimits. | C I D |
| C13. Configurar el servidor de correu i instal·lar software antispam per evitar correu brossa d'entrada. | C I D |
| C14. Actualitzacions regulars d'antivirus, antispam i altre codi maliciós. Sempre que sigui possible les actualitzacions seran automàtiques i, en cas de no ser-ho, com a mínim seran setmanals. | C I D |
| C15. Actualització de pegats de programari de correu electrònic del servidor i del sistema operatiu que el suporta. | C I D |
| C16. Activació de filtres en els servidors de correu sempre que sigui possible per restringir l'entrada d'alguns tipus de fitxer (extensions del tipus ".exe", ".sfr", ".pif", ".bat", ...). | C I D |
| C17. Configuració dels clients de correu per demanar l'acceptació de l'usuari abans d'executar un programa o script. | C I D |

### *4.4. IA – Identificació i Autenticació*

| **OBJECTIUS** | |
|---|---|
| Prevenir l'accés no autoritzat als comptes de correu electrònic.<br>Prevenir l'ús indegut de credencials d'accés. | |
| **CARACTERÍSTIQUES** | |
| **Descripció** | **Categoria** |
| C18. Tots els usuaris han de tenir un ID assignat, pel seu ús personal i exclusiu, per tal de poder exigir responsabilitats a l'usuari que en sigui responsable. Cal definir una regla de construcció dels Ids i disposar d'una llista d'Ids assignats a usuaris, que permeti establir una relació unívoca ID – usuari / persona que truca per part dels serveis de suport. | C I |
| C19. No activar per defecte les opcions de recordatori d'ID i contrasenya. | C I |
| C20. Les polítiques de contrasenya del correu han de ser raonablement segures i complir amb la *Norma contrasenyes.* | C I |
| C21. Els comptes de correu inactius (l'usuari no s'ha connectat en un temps determinat, encara que la bústia pot estar rebent correus) durant un període de 6 mesos seran desactivats. | C D |
| C22. Configurar el sistema per tal que després de 5 intents d'accés sense èxit el compte de correu quedi bloquejat durant 15 minuts. | C I |
| C23. De forma continuada i com a mínim un cop l'any, cal fer una revisió d'usuaris de correu actius per verificar que totes les persones que estan fent servir el correu estan autoritzades a fer-ho (detectar comptes no donats de baixa, ...). | C D |
| C24. Existència de procediments de notificació d'activació / desactivació de comptes de correu. Aquests procediments han de contemplar diferents nivells de notificació (normal, urgent). | C D |
| C25. La creació de llistes de distribució global (aquelles que l'usuari no pot crear localment, sinó que han de ser creades per l'administrador) ha de fer-se segons un procediment predefinit. La creació d'una llista ha de portar implícita la definició de | C I D |

| | |
|---|---|
| quines persones hi tenen accés i qui és el responsable de mantenir-la. | |
| C26. Les bústies de correu no personals (departamentals, d'àrees, serveis, organitzacions, empreses, ...), han d'anar associades a una única persona física, que serà la responsable de delegar l'accés a d'altres persones quan sigui necessari. | C I |

### *4.5. CA – Control d'accés*

| **OBJECTIUS** | |
|---|---|
| Prevenir l'ús indegut i no autoritzat del servei de correu electrònic, limitant i controlant l'accés de l'usuari al servei en funció dels drets que tingui assignats i del seu perfil.<br>Controlar els drets d'administració i monitoratge del sistema. | |
| **CARACTERÍSTIQUES** | |
| **Descripció** | **Categoria** |
| C27. Existència de procediments formals d'alta o cancel·lació de comptes d'usuari per tal de garantir l'accés al servei. | C I D |
| C28. Disposar de llistes d'usuaris per nivells d'accés autoritzats (perfil usuari, perfil administrador, ...). | C I |
| C29. Quan l'accés al correu electrònic pugui fer-se mitjançant "web-mail", caldrà garantir que es fa a través de protocol segur. | C I |
| C30. Configuració de les llistes de distribució globals per a què només siguin d'ús intern i no permetin rebre missatges des d'adreces externes de la Generalitat de Catalunya. | C I D |

### *4.6. AU – Auditoria*

| **OBJECTIUS** | |
|---|---|
| Portar a terme avaluacions regulars d'àrees vulnerables en els sistemes que intervenen en la provisió del servei, que poguessin suposar una amenaça per la seguretat, en funció de models de comportament establerts. | |
| **CARACTERÍSTIQUES** | |
| **Descripció** | **Categoria** |
| C31. Creació i anàlisi de fitxers de log. | C I D |
| C32. Registre de capçaleres i logs d'activitat de correu electrònic que circuli pels servidors de correu durant 12 mesos.<br>En cas d'emmagatzemament del contingut dels missatges, només es pot accedir al seu contingut per raons de seguretat o requeriment legal i, en tal cas, cal complir amb els procediments legals establerts (presència de la persona afectada i de la persona per aquest designada) | I D |
| C33. Establir un procediment d'investigació d'incidents i de reacció. | I D |
| C34. Pels sistemes ubicats en l'àmbit dels Serveis Centrals de la Generalitat de Catalunya, es connectarà el sistema de registre de traces del sistema de correu amb l'eina centralitzada de correlació de traces de què disposa el CTTI. Igualment caldrà guardar les traces per un període de 90 dies, garantint que no puguin ser modificades ni tant sols pels administradors del sistema. | C I D |
| C35. Pels sistemes d'altres àmbits, es connectaran a eines de correlació de traces pròpies de cada àmbit quan existeixin; de no ser així, caldrà guardar les traces durant un període mínim de 90 dies i revisar-les periòdicament per a detectar anomalies o incidències en el funcionament del sistema. | C I D |

### *4.7. DS – Disponibilitat del servei*

| **OBJECTIUS** |
|---|
| Garantir la disponibilitat i continuïtat del servei i les dades, en funció dels requeriments del negoci i prevenir atacs de denegació del servei. |
| **CARACTERÍSTIQUES** |

| Descripció | Categoria |
|---|---|
| C36. Les passarel·les de correu han de ser exclusivament per l'ús intern dels dominis de la Generalitat de Catalunya, és a dir que no es permet "open relay". S'haurà de configurar el sistema i instal·lar els controls que calguin per garantir que només s'envien cap a l'exterior correus enviats des de dominis de la Generalitat de Catalunya. | D |
| C37. Prendre les mesures adients per tal de limitar el volum de les bústies de correu i facilitar la depuració periòdica del correu (automatitzada o directament per part dels usuaris), segons els nivells de servei definits i acordats en cada cas. | D |
| C38. Planificar salvaguardes regulars de les bústies de correu. | D |
| C39. Posar a disposició dels usuaris la possibilitat d'emmagatzemar correu electrònic en una ubicació amb garanties de continuïtat, integritat i confidencialitat. | C I D |
| C40. Establir procediments d'arxivament de correus, quan les necessitats així ho requereixin (com a resultat d'una anàlisi de risc o per requeriment legal) . Aquests procediments han d'incloure el procés de guarda, així com la recuperació i les facilitats de cerca, si n'hi ha. | C I D |
| C41. Els correus de sistema per temes d'administració o incidència han de tenir un destinatari identificat, responsable de llegir-lo i actuar quan correspongui. | I D |
| C42. Configurar el servidor de manera que limiti la grandària dels missatges, però considerant possibles excepcions en funció d'usuari / rol / nivell en l'organització. | D |
| C43. En cas d'existir usuaris que, en el compliment de les seves funcions hagin de fer trameses massives de missatges, establir els procediments de comunicació quan s'escaigui entre l'usuari i l'administrador del sistema, per tal de no posar en perill la disponibilitat del servei. | D |
| C44. Qualsevol incident de seguretat haurà de ser comunicat en la major brevetat possible mitjançant el *Procediment de notificació d'incidents de seguretat.* | C I D |

### *4.8. DI – Divulgació*

| **OBJECTIUS** | |
|---|---|
| Formar i conscienciar a l'usuari en un ús correcte del servei de correu, donar a conèixer les principals amenaces i les accions i procediments per combatre-les. | |
| **CARACTERÍSTIQUES** | |
| **Descripció** | **Categoria** |
| C45. Establir i donar a conèixer un procediment de comunicació d'incidències, registre i seguiment. | C I D |
| C46. Comunicar difusió de virus o altre codi maliciós. | I D |
| C47. Comunicar a l'usuari comportaments anòmals en l'ús del correu realitzats amb les seves credencials. | C I D |
| C48. Divulgar notícies d'amenaces o atacs de seguretats perpetrats amb èxit a altres empreses o institucions i l'impacte sobre el negoci, quan sigui possible. | C I D |
| C49. Revisar els butlletins de seguretat que l'Oficina de Seguretat elabora on es recullen les vulnerabilitats detectades per a diferents sistemes. | C I D |

### *4.9. OU – Outsourcing o subcontractació del servei*

| **OBJECTIUS** | |
|---|---|
| Garantir l'acompliment de les mesures de seguretat i dels acords de nivell de servei en cas de subcontractació o externalització del servei. | |
| **CARACTERÍSTIQUES** | |
| **Descripció** | **Categoria** |
| C50. Es recollirà contractualment la llista de controls de seguretat a aplicar als sistemes de correu electrònic i a la seva administració. | C I D |
| C51. Es garantirà el compliment de la *Norma de contractació de tercers*. | C I D |

| | |
|---|---|
| C52. Garantir la qualitat i el nivell de servei requerit, a través d'acords de nivell de servei:<br>• La capacitat del sistema.<br>• La disponibilitat requerida.<br>• Els procediments d'escalat d'incidències.<br>• Els procediments de manteniment d'usuaris (alta, baixa i modificació´).<br>• El rendiment.<br>• La continuïtat del servei.<br>• Els controls de seguretat.<br>• El cost del servei.<br>L'incompliment d'acords de nivell de servei haurà de comportar penalitzacions econòmiques al proveïdor. | C I D |
| C53. Recollir contractualment les següents obligacions per part del proveïdor:<br>• Pla de recuperació en cas de desastre.<br>• Mesures de seguretat física pels equips externalitzats.<br>• Dret d'auditar al proveïdor per part del CTTI o les persones per aquesta designades. | C I D |

## 5 CONTROL

Per a l'àmbit dels Serveis Centrals de la Generalitat de Catalunya, el control del compliment d'aquesta guia es realitzarà mitjançant auditories periòdiques segons s'estableix en el *Pla d'auditories de seguretat*. Per altres àmbits, es recomana realitzar auditories cada 6 mesos.

En el cas de què no s'apliqui algun dels controls d'aquesta guia, caldrà justificar i documentar aquestes excepcions. Per a l'àmbit dels Serveis Centrals de la Generalitat de Catalunya, cada excepció a un control haurà de ser autoritzada prèviament per l'Oficina de Seguretat.

Caldrà mantenir un registre on quedin recollides totes les excepcions, a disposició de les auditories.

## 6 PENALITZACIONS

Quan l'explotació / manteniment dels sistemes estigui subcontractat, en cas d'incompliment aplicaran les penalitzacions recollides en el contracte de la prestació del servei.

Si l'administració del sistema recau en personal intern de la Generalitat de Catalunya, l'incompliment d'aquesta guia pot determinar, si s'escau, l'aplicació del règim disciplinari corresponent.

## 7 DIVULGACIÓ

El CTTI publicarà aquesta guia a la seva intranet.

Quan apliqui, l'Oficina de Seguretat serà responsable de la distribució d'aquesta guia en l'entorn de Serveis Centrals de la Generalitat de Catalunya.

## 8 REVISIÓ

Aquesta guia ha de ser revisada cada 6 mesos.

En cas de produir-se una incidència de seguretat relacionada amb aquesta guia, caldrà fer una revisió de compliment i completesa.

## 9 GLOSSARI DE TERMES

## 10 DOCUMENTACIÓ REFERENCIADA

- SC-NOR05 Norma contrasenyes.
- CT-NOR03 Norma de contractació de tercers.
- GE-PRO01 Procediment de notificació d'incidents de seguretat
- Pla d'auditories de seguretat.

**NOTA:** Quan en un determinat àmbit no existeixi la norma referenciada en aquest punt, caldrà remetre's a la guia genèrica corresponent d'àmbit Generalitat de Catalunya.

## 11 PARAULES CLAU

Correu electrònic, bústia de correu, Exchange, iPlanet, Outlook, Lotus Notes, spam, antivirus, guia, administració, controls de seguretat.

## 12 HISTÒRIC DEL DOCUMENT

Versió 1.0

Dates d'inici de cada fase:

| *Detecció de necessitat* | *Fase de treball* | *Fase de discussió* | *Fase d'aprovació* | *Fase de difusió* | *Fase de suport* |
|---|---|---|---|---|---|
| 11/2005 | 12/2005 | 03/2006 | 04/2006 | 06/2006 | 09/2006 |

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

Equip de discussió:

CTTI – Innovació i Tecnologia: J. Pérez, Ll.Coma, F. Parés, A. Massó, A. Haro, Llorenç Franco, Emili Platel, Marc Sunyer, gestors de tecnologia del CTTI

Òrgan aprovador: Comitè de Direcció del CTTI

Equip de suport: Oficina Seguretat