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 a aplicar per a la protecció de les xarxes *WiFi* amb l'objectiu de garantir la confidencialitat, integritat i disponibilitat de la informació a la qual s'accedeix a través de les xarxes sense fils.

### ÀMBIT

Xarxes *WiFi* de la Generalitat de Catalunya.

## 1 OBJECTIU

Establir els controls per administrar i gestionar les xarxes d'àrea local sense fils (*xarxes WiFi*), tant les que permeten a usuaris connectar-se als recursos de la Generalitat de Catalunya com les que permeten la connexió a Internet.

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

## 2 ÀMBIT I VIGÈNCIA

Aquesta guia va destinada als administradors i responsables de manteniment de les xarxes WiFi de la Generalitat de Catalunya. La resta de treballadors, siguin o no de la Generalitat de Catalunya, tenen prohibida la instal·lació i configuració de *xarxes WiFi*.

A més d'aquesta guia, s'hauria de complir allò que estigui establert a qualsevol altra guia d'administració de xarxes d'àrea local per cable, ja que en aquesta guia s'identifiquen els controls específics per *xarxes WiFi*.

En el cas que el manteniment de les xarxes estigui externalitzat, caldrà exigir per contracte l'aplicació dels controls de seguretat.

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
- 10.6.1 Controls de xarxa
- 10.6.2 Seguretat dels serveis de xarxa
- 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 orientats a garantir la confidencialitat, privacitat, integritat i disponibilitat de la informació, 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 una *xarxa WiFi* està exposada. En tot cas, alguns dels controls ajuden a dificultar la intrusió a la xarxa però no l'eviten al 100%. L'aplicació d'un conjunt ampli dels controls d'una manera lògica, ordenada i planificada reduirà progressivament les vulnerabilitats de la xarxa i, per tant, l'exposició als riscos. Sota la columna "categoria", s'especifiquen els aspectes de seguretat que cada control reforça (confidencialitat– C, integritat– I, disponibilitat– D).

### *3.1. CN - Configuració*

| **OBJECTIUS** | |
|---|---|
| Controls per a configurar correctament les *xarxes WiFi*. | |
| **CARACTERÍSTIQUES** | |
| **Descripció** | **Categoria** |
| C1. No fer servir el *SSID* per defecte del fabricant. | C D |
| C2. Configurar un *SSID* que no contingui informació de la Generalitat de Catalunya ni del fabricant del punt d'accés. | C D |
| C3. No configurar un *SSID* comú per tots els punts d'accés. | C D |
| C4. Inhabilitar l'emissió del *SSID* per broadcast. Això implicarà configurar el *SSID* a cadascuna de les estacions de treball (ET). | C I D |

| | |
|---|---|
| C5. No permetre que l'usuari pugui veure la *PSK* configurada en l'estació de treball. | C |

### *3.2. MN - Monitoratge*

| **OBJECTIUS** | |
|---|---|
| Registrar tots els intents d'accés a les *xarxes WiFi* per tal de poder conduir futures investigacions en cas de necessitat i atribuir-ne responsabilitats. | |
| **CARACTERÍSTIQUES** | |
| **Descripció** | **Categoria** |
| C6. Registrar accessos amb i sense èxit. | C I |
| C7. Registrar problemes i caigudes. | C I |
| C8. Instal·lar eines per rastrejar accessos no autoritzats, punts ocults i falsos punts d'accés. | C I D |

### *3.3. IA - Identificació i Autenticació*

| **OBJECTIUS** | |
|---|---|
| Identificar i autenticar correctament a l'usuari que vol accedir a una *xarxa WiFi*. | |
| **CARACTERÍSTIQUES** | |
| **Descripció** | **Categoria** |
| C9. Utilitzar un servidor d'autenticació per autenticar les connexions de les ET cap als punts d'accés. | C I D |
| C10. En cas que no es pugui utilitzar un servidor d'autenticació, utilitzar una *PSK* (una clau compartida d'accés a la xarxa WiFi) que sigui suficientment segura i robusta (mínim 20 caràcters i que no sigui una paraula de diccionari). Veure la *Norma de gestió de comptes d'administració de sistemes* per més informació. | C D |
| C11. No fer servir la contrasenya d'administració per defecte del punt d'accés. En canvi, utilitzar-ne una de més segura i robusta. Veure la *Norma de gestió de comptes d'administració de sistemes* per més informació. | C D |

### *3.4. CA - Control d'accés*

| **OBJECTIUS** | |
|---|---|
| Prevenir que persones no autoritzades puguin tenir accés a la informació i/o a les aplicacions / recursos disponibles mitjançant les *xarxes WiFi*. | |
| **CARACTERÍSTIQUES** | |
| **Descripció** | **Categoria** |
| C12. Utilitzar l'estàndard de seguretat *WPA* o *WPA2* tant al servidor d'autenticació com a les ET per assegurar l'accés només d'usuaris autoritzats i el xifrat de les comunicacions. Si fos necessari fer servir l'estàndard de seguretat *WEP*, que no és segur i ofereix una porta d'entrada per intrusos, caldrà una autorització del responsable de sistemes i/o comunicacions. | C I D |
| C13. Col·locar els punts d'accés en zones interiors dels edificis, lluny de finestres i parets exteriors, on no puguin ser manipulats per personal no autoritzat (per exemple, en prestatgeries altes o dintre d'armaris amb clau). | C D |
| C14. Reduir la potència del senyal del punt d'accés al mínim necessari per permetre les comunicacions dintre l'Organització. | C D |
| C15. Deshabilitar l'administració remota dels punts d'accés per tal d'evitar que un intrús hi pugui accedir en mode administrador des d'Internet o qualsevol altra xarxa externa. | D |
| C16. Als punts d'accés a *xarxes WiFi* que s'utilitzin únicament per connectar-se a Internet i no es requereixi autenticació, com per exemple a sales de premsa o de formació, no hi podrà haver accés a recursos de l'Organització. | C I D |
| C17. Utilitzar túnels *VPN* en cas de connexió a les *xarxes WiFi* de l'Organització des de fora de les xarxes de la Generalitat de Catalunya, com per exemple des d'Internet. | C I |

### *3.5. AU - Auditoria*

| **OBJECTIUS** | |
|---|---|
| Controlar la configuració dels punts d'accés a les *xarxes WiFi*, i analitzar esdeveniments registrats que poguessin suposar una amenaça per la seguretat, identificant àrees vulnerables. | |
| **CARACTERÍSTIQUES** | |
| **Descripció** | **Categoria** |
| C18. Per a l'àmbit dels Serveis Centrals de la Generalitat de Catalunya, l'auditoria periòdica de les *xarxes WiFi* es realitzarà segons s'estableix en el *Pla d'auditories de seguretat*. Per altres àmbits, es recomana realitzar auditories cada 6 mesos. | I D |

### *3.6. DS - Disponibilitat del servei*

| **OBJECTIUS** | |
|---|---|
| Garantir la disponibilitat i continuïtat de les *xarxes WiFi* en funció dels requeriments del negoci. | |
| **CARACTERÍSTIQUES** | |
| **Descripció** | **Categoria** |
| C19. Els punts d'accés a les *xarxes WiFi* han de tenir un servei de manteniment contractat segons les necessitats del negoci. El contracte de manteniment hauria de contemplar la substitució d'aquests dispositius en cas de necessitat. | I D |
| C20. Tenir fàcil accessibilitat a informació de proveïdors, com per exemple informació de contacte (responsables, telèfons i adreces), contractes, acords vigents, etc. | D |
| C21. Deshabilitar el servei DHCP als punts d'accés si no és necessari. | D |
| C22. S'ha de mantenir actualitzat el firmware dels punts d'accés, així com els controladors d'aquests dispositius. | C I D |
| C23. 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 |

### *3.7. DI - Divulgació*

| **OBJECTIUS** | |
|---|---|
| Formar i conscienciar a l'usuari en un ús correcte de les *xarxes WiFi*. | |
| **CARACTERÍSTIQUES** | |
| **Descripció** | **Categoria** |
| C24. Donar a conèixer el *Procediment de gestió d'incidències*. | C I D |
| C25. Comunicar a l'usuari comportaments anòmals en l'accés a les *xarxes WiFi* amb les seves credencials. | C I D |
| C26. Divulgar notícies d'amenaces o atacs de seguretat perpetrats amb èxit a les *xarxes WiFi* d'altres empreses o institucions i l'impacte sobre el negoci, quan sigui possible. | C I D |
| C27. Comunicar la prohibició de crear *xarxes WiFi* no autoritzades. | C I D |
| C28. Comunicar la prohibició de connectar-se a altres *xarxes WiFi* no controlades, mentre s'estigui connectat a la de l'organització per evitar obrir la xarxa a tercers | C I D |

### *3.8. 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 de manteniment de les *xarxes WiFi*. | |
| **CARACTERÍSTIQUES** | |
| **Descripció** | **Categoria** |
| C29. Recollir contractualment la llista de controls de seguretat a aplicar a les *xarxes WiFi* i la seva administració. | C I D |
| C30. Garantir el compliment de la *Norma de contractació de Tercers*. | C I D |

| | |
|---|---|
| C31. Garantir la qualitat i el nivell de servei requerit, a través d'acords de nivell de servei:<br>• Procediments d'escalat d'incidències.<br>• Temps de resolució d'incidències.<br>• Temps de resposta per canvis / noves instal·lacions.<br>• Compliment i actualització dels controls de seguretat.<br>• Gestió de problemes.<br>• ...<br>L'incompliment d'acords de nivell de servei haurà de comportar penalitzacions econòmiques al proveïdor. | 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

*PSK:* Pre-shared Key, és un conjunt de caràcters que es faran servir per xifrar les comunicacions entre l'ET i el punt d'accés a la xarxa WiFi.
*SSID:* Service Set Identifier, és un conjunt de caràcters que identifiquen una xarxa WiFi i la distingeix de les altres.
*VPN*: Virtual Private Network, xarxa privada virtual mitjançant la qual un usuari pot connectar-se de manera segura (amb autenticació i on la informació serà xifrada) a la xarxa interna de l'Organització des d'Internet o qualsevol altra xarxa insegura.
*WEP:* Wired Equivalent Privacy, és un sistema de securització de xarxes WiFi ja obsolet per les múltiples vulnerabilitats de seguretat que presenta.
*WPA:* WiFi Protected Access, és un sistema de securització de xarxes WiFi que substitueix al WEP i que està basat en l'estàndard IEEE 802.11i. Introdueix un nou sistema de xifrat (TKIP) que augmenta la confidencialitat i la integritat de les dades en les comunicacions.
*WPA2:* WiFi Protected Access 2, és una nova versió de WPA que implementa completament l'estàndard de seguretat IEEE 802.11i. Utilitza un sistema de xifrat anomenat AES que introdueix importants millores en les comunicacions xifrades.
*Xarxa WiFi:* Xarxa d'àrea local a la qual la transmissió de la informació es fa per ones de ràdio a una determinada freqüència, entre diversos dispositius un dels quals és un punt d'accés a d'altres xarxes. Les comunicacions s'estableixen en base a l'estàndard de comunicacions IEEE 802.11.

## 10 DOCUMENTACIÓ REFERENCIADA

- SC-NOR07 Norma de gestió de comptes administrador sistemes
- 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

Xarxa, punt d'accés, estació de treball (ET), guia, administració, WiFi, Wireless, xarxa inalàmbrica.

## 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* |
|---|---|---|---|---|---|
| 09/01/2006 | 06/02/2006 | 06/03/2006 | 03/04/2006 | 01/06/2006 | 01/09/2006 |

Equip de treball: Qualitat i Seguretat: Silvia Garre, Josep Mangas, Oficina Seguretat (Indra)
Equip de discussió:
CTTI – Innovació i Tecnologia: Emili Platel, Joan Pérez, Marc Sunyer, Llorenç Coma, Llorenç Franco, Albert Haro.
CTTI – Radiotelecomunicacions i desplegament d'infraestructures de comunicacions: Lluís Guillén
Òrgan aprovador: Comitè de Direcció del CTTI
Equip de suport: Oficina Seguretat