ÍNDEX

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

Estàndard signat digitalment pel:
Generalitat de Catalunya

Centre de Telecomunicacions i Tecnologies de la Informacio
Estàndard aprovat
Barcelona
2007.03.13 13:42:15 +01'00'

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

RESUM

OBJECTIU

Definir els controls de seguretat que cal aplicar a les estacions de treball (ET) de la Generalitat de Catalunya, per tal de protegir i garantir la integritat, confidencialitat, privacitat i disponibilitat de la informació que emmagatzemen o a la que des d'aquestes s'hi pot accedir, facilitar el manteniment i gestió del parc informàtic i garantir l'acompliment de la legislació vigent.

ÀMBIT

Estacions de treball de la Generalitat de Catalunya.

1 OBJECTIU

Definir els controls de seguretat que cal aplicar a les estacions de treball (ET) de la Generalitat de Catalunya, per tal de protegir i garantir la integritat, confidencialitat, privacitat i disponibilitat de la informació que emmagatzemen o a la que des d'aquestes s'hi pot accedir, facilitar el manteniment i gestió del parc informàtic i garantir l'acompliment de la legislació vigent.

2 ÀMBIT

Aquesta guia va destinada als administradors i responsables de manteniment de les ET 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 establir les solucions tecnològiques per la implantació de cada tipus de control.

S'entén per ET qualsevol equip a través del qual l'usuari accedeix habitualment a la informació, aplicacions i sistemes d'informació necessaris pel desenvolupament habitual de les funcions encomanades.

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

Entrarà en vigor el dia xx d'Octubre 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 per una ET, 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 ET està exposada. Sota la columna "categoria", s'especifiquen els aspectes de seguretat que cada control reforça (confidencialitat– C, integritat– I, disponibilitat– D).

3.1. MN - Monitoratge

OBJECTIUS	
Registrar tots els intents d'accés a l'estació de treball, els canvis de configuració, ... per tal de poder conduir futures investigacions en cas de necessitat i atribuir-ne responsabilitats.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C1. Registrar accessos amb i sense èxit.	C I
C2. Registrar problemes i caigudes.	C I
C3. Instal·lar eines per rastrejar canvis de configuració.	C I D

3.2. FI - Fiabilitat de les dades

OBJECTIUS
Protegir la integritat de la informació de l'ET.

CARACTERÍSTIQUES		
	Descripció	**Categoria**
C4.	Instal·lació d'antivirus que s'activin en l'arranc de l'ET, en l'accés en mode lectura a dispositius de memòria i en l'obertura de fitxers. Actualitzacions regulars de l'antivirus, com a mínim setmanals.	C I D
C5.	Instal·lació de pegats de sistema operatiu per a solucionar les vulnerabilitats de seguretat detectades pel fabricant.	C I D
C6.	Configurar els navegadors i clients de correu electrònic per demanar l'acceptació de l'usuari abans d'executar un programa o script.	C I D
C7.	Instal·lació del programari d'assistència remota en cas que s'utilitzi a l'Organització, i configuració d'aquest per a què demani sempre l'acceptació de l'usuari.	C I D
C8.	Procediment de protecció d'ET (tallafocs, xifrat, ...). Establir polítiques sobre qui hauria de tenir una estació de treball securitzada i definir el procediment de sol·licitud de securització de l'ET.	C I

3.3. I&A - Identificació i Autenticació

OBJECTIUS		
Identificar i autenticar correctament a l'usuari que vol accedir a una ET.		
CARACTERÍSTIQUES		
	Descripció	**Categoria**
C9.	Les estacions de treball han de tenir configurat per defecte l'accés a través d'un mitjà d'autenticació segur, com a mínim identificador d'usuari i contrasenya, i complir amb la *Norma de contrasenyes*. Aquest punt és especialment important per dispositius mòbils (PDA, agenda electrònica, ...).	C I
C10.	No visualitzar l'identificador d'usuari de l'última sessió a la pantalla, i protegir la contrasenya per què no aparegui en pantalla.	C I
C11.	Configurar el sistema per a què forci el canvi de contrasenya per part de l'usuari la primera vegada que hi accedeix i també de forma periòdica, impedint la reutilització de les últimes contrasenyes, segons estipuli la *Norma de Contrasenyes*.	C I
C12.	Possibilitat d'acceptar altres sistemes d'autenticació: certificat digital, biometria, ...	C I

3.4. CA - Control d'accés

OBJECTIUS		
Prevenir que persones no autoritzades puguin accedir a la informació continguda a l'ET i/o a les aplicacions / recursos disponibles des de l'ET.		
CARACTERÍSTIQUES		
	Descripció	**Categoria**
C13.	Previ a l'autenticació de l'usuari cal mostrar un missatge advertint de què el sistema al que s'està accedint és per ús exclusiu de la Generalitat de Catalunya i que no està permès l'accés sense autorització. Abans de continuar el procés d'autenticació, l'usuari ha d'acceptar el missatge.	C
C14.	Configurar l'arranc de les estacions de treball des de la unitat de disc configurada com a partició primària d'arranc, amb BIOS bloquejada, per evitar l'activació d'altres dispositius d'arranc (disquets, CD-Rom, Wake-On-Lan, ...).	C I
C15.	Definir polítiques de control de les operacions permeses segons el perfil de l'usuari: arranc d'aplicacions, accés a recursos locals i remots, accés al set-up del sistema, instal·lació / desinstal·lació de programari o maquinari, configuració de drivers de dispositiu i maquinari perifèric, configuració de serveis de xarxa, mòdem, ...	C I
C16.	Donar les autoritzacions en funció del rol i necessitats de l'usuari. No es donaran accessos d'administrador local sobre les ET per defecte. Si es requereix aquest tipus d'accés, ha de ser controlat per l'administrador de la xarxa.	C I
C17.	Activació de mecanismes de bloqueig de pantalla al cap d'un cert temps d'inactivitat (recomanable entre 5 i 10 minuts), de manera que calgui tornar autenticar-se per accedir novament a l'ET.	C I

C18. Desactivació de tots els ports/serveis que estiguin actius i no siguin necessaris.	C I D

3.5. RO - Reutilització d'objectes

OBJECTIUS	
Controlar la correcta reutilització o eliminació de les ET.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C19. Procediment de retirada d'equips del parc per obsolescència (esborrat de tota la informació del disc local de manera segura, eliminació de tot el programari instal·lat sota llicència, revisió de què no existeix cap suport extern a l'equip, actualització inventari programari i maquinari, actualització assegurança, ...).	C I
C20. Procediment de reutilització o reciclatge d'equips (esborrar tota la informació del disc local de manera segura, restablir la configuració inicial estàndard d'ET, ...).	C I D

3.6. AU - Auditoria

OBJECTIUS	
Controlar la configuració de les ET, i analitzar esdeveniments registrats que poguessin suposar una amenaça per la seguretat, identificant àrees vulnerables.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C21. Definició d'uns estàndards mínims d'ET que estiguin documentats i actualitzats (configuració inicial, dispositius que incorpora per defecte, programari instal·lat de partida, mesures de seguretat, etiquetatge d'equips, imatge corporativa si existeix, ...).	I D
C22. Documentar els procediments d'instal·lació, configuració i manteniment dels equips. Les accions de manteniment haurien d'incloure l'esborrat de programari no autoritzat, tot i que es recomana avisar prèviament l'usuari.	I D
C23. Rastreig a intervals de temps prefixats, d'àrees potencialment vulnerables: • Revisió del sistema operatiu (usuaris, grups, sistema de fitxers, configuració del sistema i els serveis, contrasenyes, compartició de recursos, ...). • Presència d'aplicacions no autoritzades i cavalls trojans. • Presència de connexions remotes no autoritzades.	C I A
C24. Verificació de la integritat de fitxers crítics emmagatzemats en local.	I

3.7. DS - Disponibilitat del servei

OBJECTIUS	
Garantir la disponibilitat i continuïtat de l'ET i aplicacions locals, en funció dels requeriments del negoci.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C25. Les ET han de tenir un servei de manteniment contractat segons les necessitats del negoci. El contracte de manteniment hauria de contemplar la substitució d'una ET en cas de necessitat, restablint la informació continguda a partir de l'última còpia de seguretat.	I D
C26. Procediments i dispositius per fer backup del disc local.	I D
C27. Procediments de backup sobre la xarxa.	I D
C28. Procediment de sol·licitud de substitució / nou maquinari.	D
C29. Procediment de sol·licitud de nou programari.	D
C30. Accessibilitat a informació de proveïdors: de contacte, contractes, acords vigents, ...	D
C31. Qualsevol incident de seguretat amb les ET haurà de ser comunicat en la major brevetat possible mitjançant el *Procediment de notificació d'incidents de seguretat.*	C I D

3.8. DI - Divulgació

OBJECTIUS	
Formar i conscienciar a l'usuari en un ús correcte de l'ET.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C32. Establir i donar a conèixer un procediment de comunicació d'incidències, registre i seguiment.	C I D
C33. Comunicar difusió de virus o altre codi maliciós.	I D
C34. Comunicar a l'usuari comportaments anòmals en l'accés a l'ET amb les seves credencials.	C I D
C35. Divulgar notícies d'amenaces o atacs de seguretat perpetrats amb èxit a altres empreses o institucions i l'impacte sobre el negoci, quan sigui possible.	C I D

3.9. 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 de manteniment de les ET.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C36. Recollir contractualment la llista de controls de seguretat a aplicar a les ET i la seva administració.	C I D
C37. Garantir el compliment de la *Norma de contractació de tercers*.	C I D
C38. Garantir la qualitat i el nivell de servei requerit, a través d'acords de nivell de servei: • Procediments d'escalat d'incidències. • Temps de resolució d'incidències. • Temps de resposta per canvis / noves instal·lacions. • Compliment i actualització dels controls de seguretat. • Gestió de problemes. • ... L'incompliment d'acords de nivell de servei haurà de comportar penalitzacions econòmiques al proveïdor.	C I D
C39. Recollir contractualment les següents obligacions per part del proveïdor: • Compliment de la legislació vigent, especialment en el que respecta al tractament de dades personals. • Compliment de normatives de l'Organització per part del proveïdor i el seu personal. • Actuació esperada i responsabilitats en cas de desastre.	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 de les ET estigui subcontractat, en cas d'incompliment aplicaran les penalitzacions recollides en el contracte de la prestació del servei.

Si l'administració de les ET 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.

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 com a mínim anualment.

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

- CT-NOR03 Norma de contractació de tercers
- SC-NOR05 Norma de contrasenyes
- 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

Estació de treball, ordinador, portàtil, 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*
6/2005	9/2005	4/2006	10/10/2006	13/10/2006	1/1/2007

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

Equip de discussió:

1a revisió (juny 2005): AE (JI. Grau, A.Inarejos) IiT (X.Milà, J.Pérez, A.Haro, A.Massó, Ll.Coma i alguns gestors tecnològics, T.Escuín, F.Parés), AC (J.Gabaldá, 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 arquitectures), 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