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: Silvia Garre (CTTI – Qualitat i Seguretat)

Estàndard signat digitalment pel:

Generalitat de Catalunya

Centre de Telecomunicacions i Tecnologies de la Informacio
Estàndard aprovat
Barcelona
2006.12.20 19:24:29 +01'00'

RESUM

1. Objectiu: Elaborar una guia de connexió d'equips de tercers a la xarxa interna, que recull els requeriments que han de complir els externs i els seus equips, quan es connecten a la xarxa interna de l'organització.

Condició prèvia a la connexió dels equips a la xarxa: compliment per part del responsable de la contractació de possibles normes de contractació de tercers, i signatura per part dels externs document d'acceptació d'obligacions relatives a seguretat de la informació i protecció de dades de caràcter personal, quan existeixi (consultar com a exemple *CT-NOR03 Norma de contractació de tercers al CTTI*).

2. Àmbit: Ordinadors i altres dispositius electrònics que personal de tercers contractat per l'*organització* utilitzi durant la prestació dels seus serveis a l'*organització,* per la connexió a la xarxa interna de l'*organització* o a qualsevol altra xarxa de la Generalitat de Catalunya.
Equips de propietat que els treballadors interns vulguin connectar a la xarxa interna.

3. Descripció:

- Protecció de la informació (sol·licitud d'accés, protecció de contrasenyes, emmagatzemament de la informació, xifrat d'informació, bloqueig de l'estació de treball, extracció d'informació, ...).
- Tractament d'incidències.
- Configuració dels equips (requeriments del sistema operatiu, protecció contra codi maliciós, prohibició d'alterar la configuració predefinida, d'instal·lació de programari, de configuració de dispositius de comunicacions, programari contra codi maliciós, configuracions prohibides, programari no autoritzat, ...).

1. OBJECTIU I MOTIVACIÓ

La subcontractació de serveis a tercers, i la necessitat d'aquests tercers de treballar dins la xarxa de l'organització, fa necessària l'emissió d'unes normes a complir quan es permeti la connexió d'equips de tercers a la xarxa interna.

Aquesta guia té dos objectius primordials:

- Protegir la confidencialitat, integritat i disponibilitat de la informació de la Generalitat de Catalunya, a la qual s'accedeix a través d'aquests equips, així com el compliment de la legislació vigent en matèria de seguretat de la informació.
- Garantir un bon funcionament de la infraestructura informàtica i de comunicacions de l'organització.

Previ a la connexió dels equips a la xarxa interna, el responsable de la contractació del servei haurà de complir la *"Guia de contractació de tercers".*

2. ÀMBIT I VIGÈNCIA

Aquesta guia és d'aplicació per tots els ordinadors i altres dispositius electrònics que personal de tercers utilitzi durant la prestació dels seus serveis a l'organització, per la connexió a la xarxa interna de l'organització o a qualsevol altra xarxa de la Generalitat de Catalunya.

Quan el personal intern de l'organització vulgui connectar a la xarxa interna equips de la seva propietat, aquests rebran el mateix tractament que els equips de tercers i quedaran per tant subjectes a aquesta guia.

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:

- 6.2.1 Identificació dels riscos relacionats amb terceres parts
- 6.2.3 Requeriments de seguretat en els acords amb les terceres parts
- 10.4.1 Controls contra codi maliciós
- 11.1.1 Política de control d'accés
- 11.2.1 Registre d'usuaris
- 11.3.2 Equips d'usuari desatesos
- 11.5.2 Identificació i autenticació d'usuaris
- 11.6.1 Restricció d'accés a la informació
- 12.5.4 Fuga d'informació
- 13.1.1 Notificar dels esdeveniments de seguretat

4. DESCRIPCIÓ

Protecció de la informació

N1. Qualsevol sol·licitud d'alta, baixa o manteniment de l'accés dels usuaris externs a la xarxa ha de ser cursada pels mitjans establerts a través del responsable de l'execució del contracte dins l'organització, o la persona per aquest designada.

N2. En arrencar l'ordinador, la xarxa sol·licitarà l'autenticació de la persona que es connecta, mitjançant identificador d'usuari i contrasenya, o procediments alternatius d'autenticació segura. És responsabilitat de l'usuari complir la *Guia de contrasenyes*, especialment en els aspectes de confidencialitat i seguretat de la paraula de pas.
Quan l'autenticació es faci mitjançant procediments alternatius d'autenticació segura (certificats, tokens,...), l'usuari és responsable de fer un ús segur d'aquests mitjans d'autenticació.

N3. El principal recurs d'emmagatzematge serà sempre la unitat de xarxa habilitada per l'administrador, que serà degudament notificada al personal de l'empresa contractista. Per tant, per evitar accessos indeguts, duplicitats d'informació, facilitar la compartició d'informació i garantir la continuïtat d'aquesta informació, sempre que sigui possible s'evitarà emmagatzemar informació al disc local i en suports externs.

En qualsevol cas, l'espai de xarxa habilitat per l'organització només es farà servir per emmagatzemar informació relacionada amb el servei que s'estigui prestant.

N4. En cas que sigui indispensable emmagatzemar informació en el disc local o suports externs, caldrà prendre les mesures adequades per protegir la informació segons el nivell de confidencialitat o criticitat d'aquesta, protegint-la sempre d'accessos il·legítims. En aquest cas és responsabilitat de l'usuari garantir la continuïtat d'aquesta informació.
Qualsevol informació confidencial o afectada per la llei de protecció de dades personals ha de ser encriptada abans de ser emmagatzemada en local o en suports externs. En el cas de dades de caràcter personal, el responsable del fitxer ha d'autoritzar prèviament l'emmagatzemament en local o en suport extern.

N5. Quan l'ordinador estigui connectat a la xarxa, l'accés al correu electrònic de la companyia externa o a comptes de correu personal només es podrà realitzar a través de webmail. No està permesa la configuració d'un compte d'accés a correu extern en el programari de correu instal·lat a l'equip de treball.

N6. El personal de l'empresa contractista haurà de tenir màxima cura en el tractament de la informació que imprimeixi en paper, cuidant de deixar sempre la documentació recollida en finalitzar la jornada laboral.
Quan les dades tractades siguin confidencials o privades, protegides per la legislació de protecció de dades personals, l'empresa contractista podrà demanar un lloc segur per guardar aquesta documentació.

N7. L'ordinador no ha de quedar mai desatès, especialment si s'ha superat el procés d'identificació i autenticació per accedir a sistemes i/o aplicacions. Quan la persona connectada hagi d'abandonar l'ordinador temporalment, caldrà bloquejar l'ordinador.

N8. Cal desconnectar l'ordinador en finalitzar la jornada laboral.

N9. *[Cada organització haurà d'indicar quina és el seu criteri de connexió dels equips d'usuari als stemes d'alimentació ininterrompuda – SAI -)]*.

N10. Quan s'utilitzin ordinadors portàtils en llocs públics, sales de reunions, o altres àrees fora del lloc de treball habitual, cal prendre les mesures adients per evitar que persones alienes puguin visualitzar o accedir a la informació de l'ordinador, sense autorització.

N11. Sempre que sigui possible, connectar l'ordinador a elements fixes a través de cablejat. En absències perllongades (vacances, permisos, ...) del personal, durant les quals l'ordinador no hagi de ser utilitzat per altres persones, l'ordinador hauria de quedar guardat de forma segura.

Tractament d'incidències

N12. En cas de danys en l'ordinador, robatori o pèrdua a les instal·lacions de l'organització, cal informar immediatament a *(especificar telèfon / persona de contacte)*.

N13. Qualsevol infecció o mal funcionament de l'ordinador haurà de ser comunicada immediatament segons el *Procediment de notificació d'incidents de seguretat.*

Configuració dels equips

N14. El sistema operatiu haurà de tenir suport i manteniment del fabricant.

N15. Tot el SW que ho requereixi haurà d'estar instal·lat sota llicència vàlida.

N16. Quan l'equip no treballi en xarxa és obligatori activar localment un estalvi de pantalla que sol·liciti contrasenya i que s'activi després d'un temps d'inactivitat (es recomana entre 5 i 10 minuts).

N17. L'equip de treball haurà de tenir instal·lat un tallafocs, programari antivirus, eines de neteja de malware / spyware i política activa de pegats. Les actualitzacions d'antivirus es realitzarn periòdicament i com a mínim setmanalment. L'antivirus s'haurà d'executar automàticament en el moment de l'arranc, quan s'accedeix en mode lectura a dispositius de memòria externs (disquets, CDs, DVDs, memòries USB, ...), o quan s'intenti obrir qualsevol fitxer.

N18. Els equips de treball connectats a la xarxa, no poden, si no existeix una autorització per escrit de l'organització, ser configurats per realitzar funcions de servidor, com per exemple:

a. Servidor web o servidor web segur.
b. Servidor de correu electrònic.
c. Servidor Proxy.
d. Servidor FTP.
e. Servidor DNS.
f. Servidor DHCP.
g. Servidor de notícies (news).

h. Servidor NTP.
i. Servidor NFS o compartició de disc per NetBios.
j. Servidor de base de dades (SGBD).
k. Servidor Telnet, SSH o Terminal Server.
l. Qualsevol altre servei que pugui afectar la seguretat dels sistemes.

N19. En cap cas, tret d'autorització per escrit de l'organització, els equips de treball podran tenir instal·lades els següents tipus d'aplicacions / equips:
a. Programari de reenviament anònim.
b. Sniffers.
c. Eines per descobrir contrasenyes.
d. Escaneig de xarxa.
e. Programari peer to peer (p2p).
f. Eines per fer atacs que comprometin la seguretat dels sistemes.
g. Programari per xat, IRC, ICQ o missatgeria instantània.

N20. No es podran configurar en els equips màquines virtuals, ni instal·lar dispositius de xarxa en mode promiscu.

N21. No es podrà establir comunicació via mòdem, bluetooth o dispositius inalàmbrics sense una autorització prèvia de l'organització.

5. CONTROL

Per raons de seguretat i rendiment, la Generalitat de Catalunya es reserva el dret de:

- Mantenir traces de les relacions entre els identificadors d'usuari i les accions portades a terme en els sistemes informàtics. Aquestes traces es podrien utilitzar com a prova en cas d'accions judicials.
- Realitzar auditories sobre els ordinadors sense previ avís, en els següents casos:
  - Per sospita de què l'equip pugui estar causant problemes de rendiment o mal funcionament dels diferents elements que configuren la infraestructura informàtica i/o de comunicacions.
  - Per comprovar que s'estan complint les mesures de seguretat requerides en aquesta guia.

En el cas de què no s'apliqui alguna de les normes, caldrà justificar i documentar aquestes excepcions.

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

6. PENALITZACIONS

En cas de què l'organització detecti que els equips no compleixen les mesures de seguretat requerides, podrà desconnectar l'equip de la xarxa de forma immediata.

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

Si l'incompliment és per part de personal intern de la Generalitat de Catalunya pot determinar, si s'escau, l'aplicació del règim disciplinari corresponent.

7. DIVULGACIÓ

El CTTI publicarà aquesta guia a la seva intranet.

8. REVISIÓ

Aquesta guia es revisarà anualment.

9. GLOSSARI DE TERMES

10. DOCUMENTACIÓ REFERENCIADA

- CT-NOR03 Norma de contractació de tercers al CTTI.
- GE-GUI19 Guia de contrasenyes.
- GE-PRO01 Procediment de notificació d'incidents de seguretat.

11. PARAULES CLAU

Connexió d'equips, tercers, empresa contractista, subcontractats, xarxa interna, ...

12. HISTÒRIC DEL DOCUMENT

Versió 1.0
Redacció inicial del document

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	7/2005	9/2005	2/2006	6/2006	9/2006

Equip de treball: Qualitat i Seguretat: Silvia Garre, Josep Mangas, Oficina Seguretat (Indra)
Equip de discussió:
Assessoria estratègica: Joan Ignasi Grau, Alicia Inarejos
Atenció Client: Jordi Gabaldà, Pere Solà
Desenvolupament corporatiu i ètica: Lluís Olivé
Innovació i Tecnologia: Xavier Milà, Joan Pérez, Francesc Parés, Albert Haro, Agustí Massó, Llorenç Coma (+ gestors tecnològics), Toni Escuín, Emili Platel, Llorenç Franco, Marc Sunyer
Comunicació: Esther Roure
Assessoria Jurídica: Josep Manuel Prats
Relació amb Proveïdors: Andreu Rami
Òrgan aprovador: Comitè de Direcció del CTTI
Equip de suport: CTTI (Oficina Seguretat – Indra)