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 4
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 (guia).	CTTI – Qualitat i Seguretat	Comitè de Direcció del CTTI	26/9/2006	28/9/2006
1.0 (norma)	CTTI – Qualitat i Seguretat	Comitè Operatiu del CTTI	4/5/2009	18/5/2009

Estàndard signat digitalment pel:

Generalitat de Catalunya

Centre de Telecomunicacions i Tecnologies de la Informacio
Estàndard aprovat
Barcelona
2009.05.18 10:22:37 +02'00'

RESPONSABLE DEL DOCUMENT: CTTI – Qualitat, Seguretat i Relació amb Proveïdors

RESUM

1. Objectiu: Definir el conjunt de mesures i normes de seguretat que és obligatori complir per a qualsevol connexió que es faci a través del nus corporatiu de la Generalitat de Catalunya i per a qualsevol accés que es faci a un servei o sistema ubicat dins del nus.

2. Àmbit: Aquesta norma va dirigida a tota persona, departament, organisme o empresa contractista que faci ús de sistemes o serveis corporatius ubicats dins del nus corporatiu de la Generalitat de Catalunya o que requereixi la connexió al nus.

4. Descripció:

- Normes generals de seguretat
- Compliment d'altres normes vigents
- Administració remota de sistemes
- Assistència remota
- Transferència remota de fitxers
- Publicació a Internet
- Accés a serveis corporatius i plataformes departamentals
- Gestió de nous projectes
- Arquitectura de sistemes
- Gestió del canvi
- Connexió permanent al nus corporatiu de xarxes externes de terceres empreses

1. OBJECTIU I MOTIVACIÓ

L'objectiu d'aquest document és definir el conjunt de mesures i normes de seguretat que és obligatori complir per a qualsevol connexió que es faci a través del nus corporatiu de la Generalitat de Catalunya i per a qualsevol accés que es faci a un servei o sistema ubicat dins del nus. També es defineix la gestió i l'ús que s'ha de realitzar dels sistemes o serveis ubicats als Serveis TIC Centrals de Caràcter Continuat de la Generalitat de Catalunya gestionats pel CTTI (d'ara endavant "*Serveis TIC Centrals*").

Aquestes normes són les mínimes exigides per garantir la confidencialitat, privacitat, integritat i disponibilitat dels sistemes ubicats dins del nus, així com de la informació que s'hi troba emmagatzemada.

Algunes de les mesures de seguretat citades en aquest document, estan desenvolupades en altres guies / normes aprovades pel CTTI, a les quals es fa referència al llarg d'aquest document.

2. ÀMBIT I VIGÈNCIA

Aquesta norma va dirigida a tota persona, departament, organisme o empresa contractista que faci ús de sistemes o serveis corporatius ubicats dins del nus corporatiu de la Generalitat de Catalunya o que requereixi la connexió al nus, així com a tots els proveïdors dels *Serveis TIC Centrals.*

La norma N29, pels serveis de hosting, només serà d'aplicació per a aquells proveïdors de *Serveis TIC Centrals* amb els quals es formalitzi relació contractual després de l'entrada en vigor d'aquesta norma, tot i que es recomana fortament l'adequació a aquest control dels serveis en funcionament el més aviat possible.
La norma N29 pel servei de housing serà d'aplicació per qualsevol servei contractat després de l'entrada en vigor d'aquesta norma, tot i que es recomana fortament l'adequació a aquest control dels serveis en funcionament el més aviat possible.

Correspon a l'adaptació a norma de la guia GE-GUI28-01 Guia de mesures de seguretat al Nus Corporatiu TIC de la Generalitat, que va entrar en vigor el dia el dia 28 de setembre de 2006 i a la qual substitueix.

Data d'entrada en vigor: 18 de maig de 2009.

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

3. COMPLIMENT AMB ELS REQUISITS LEGALS I ESTÀNDARDS DE SEGURETAT

La present norma proporciona cobertura a aspectes recollits en els següents controls de la ISO 27002:2005:

- 6.2.3 Requeriments de seguretat en els acords amb les terceres parts
- 10.1.2 Gestió dels canvis
- 10.1.4 Segregació d'entorns
- 10.2.1 Prestació del servei
- 10.4.1 Controls contra codi maliciós
- 10.6.1 Controls de xarxa
- 10.6.2 Seguretat dels serveis de xarxa
- 10.8.1 Polítiques i procediments per a l'intercanvi d'informació
- 10.10.1 Registres d'auditoria (logging)
- 11.4.1 Política d'ús dels serveis de xarxa
- 11.4.2 Autenticació d'usuari per les connexions externes
- 11.4.5 Segregació a les xarxes
- 11.4.6 Control de connexió a la xarxa
- 11.5.1 Processos de connexió segurs
- 11.6.2 Aïllament de sistemes sensibles
- 12.1.1 Anàlisi i especificació dels requeriments de seguretat
- 12.2.3 Integritat dels missatges
- 13.1.1 Notificar dels esdeveniments de seguretat

4. DESCRIPCIÓ

Normes generals

N1. L'accés a qualsevol servei ha d'estar controlat mitjançant la limitació de les adreces IP origen i destí, i la delimitació d'accés als ports estrictament necessaris per a la prestació del servei. En cas de necessitar un accés no restringit a nivell d'adreces IP o de ports (accés tipus "any"), caldrà que sigui autoritzat per l'Oficina de Seguretat.

N2. No es permet l'ús *d'eines o protocols insegurs*[1] a través del nus corporatiu, sempre i quan hi hagi una alternativa segura (xifrada).

En el *Manual d'eines per comunicacions segures en el nus corporatiu de la Generalitat de Catalunya* es pot trobar un recull de recomanacions i mètodes per a protegir les comunicacions a través d'alguns protocols i serveis que no tenen suport per al xifrat.

N3. Els tercers[2] no poden accedir a cap sistema a través d'*eines o protocols insegurs*, ni tan sols quan aquest accés es realitzi via VPN.

Compliment d'altres normes vigents

N4. Quan la gestió d'un sistema estigui subcontractada o externalitzada, és obligatori entregar totes les normes, guies i procediments de seguretat vigents que li siguin d'aplicació a l'empresa contractista. S'haurà d'incloure en l'elaboració de tots els plecs de contractació els annexes de requeriments de seguretat que corresponguin. És responsabilitat de la persona responsable a nivell Generalitat, el fer arribar aquesta documentació al tercer[2].

N5. Per a la definició i gestió de les contrasenyes dels comptes, caldrà aplicar la *Norma de gestió de comptes d'administració de sistemes* i la *Norma de contrasenyes*.

N6. És obligatori complir les guies de protecció *(hardening)* per a tots els sistemes així com la resta d'estàndards d'obligat compliment en l'àmbit dels *Serveis TIC Centrals*.

N7. Cal complir la *Norma de connexió d'equips de tercers* quan sigui necessari connectar equips de tercers al nus corporatiu.

N8. Qualsevol incident de seguretat haurà de ser comunicat en la major brevetat possible mitjançant el *Procediment de notificació d'incidents de seguretat.*

Administració remota de sistemes

N9. No es poden fer tasques d'administració remota amb *eines o protocols insegurs* a través del nus corporatiu (com per exemple: *TELNET*, X-Windows, XDMCP, rexec, rlogin etc. o RDP/PcAnywhere/VNC/DameWare sense xifrar). La comunicació es farà sempre de forma xifrada.

Es recomana l'ús de les eines gràfiques especificades en el *Manual d'eines per comunicacions segures en el nus corporatiu de la Generalitat de Catalunya* per a la realització de tasques d'administració remota. Aquestes eines, configurades de forma correcta, ofereixen tots els controls de seguretat i compleixen totes les normes especificades en aquest document.

Es recomana per simplicitat, fiabilitat i compatibilitat l'ús de Secure Shell (SSH) per a l'administració per consola remota. En el *Manual d'eines per comunicacions segures en el nus corporatiu de la Generalitat de Catalunya* es poden trobar exemples de programaris recomanats per la seva àmplia utilització en els sistemes d'informació.

N10. L'accés de tercers[2] per a administració d'equips s'ha de fer via VPN.

Assistència remota

N11. No es poden fer tasques d'assistència remota amb *eines o protocols insegurs* a través del nus corporatiu (com per exemple RDP/PcAnywhere/ DameWare sense xifrar, etc.). La comunicació es farà sempre de forma xifrada.

[1] En aquest context es consideren insegurs aquelles eines o protocols que transmeten informació confidencial o privada (com ara noms d'usuari i contrasenyes) en clar per la xarxa

[2] S'enten com a tercer el personal extern que presti serveis a la Generalitat de Catalunya

N12. Només es podrà realitzar tasques d'assistència remota en equips on l'usuari tingui la sessió activa i hi sigui present. L'usuari haurà d'acceptar la connexió, podrà seguir totes les actuacions i podrà finalitzar la connexió en tot moment. Un cop finalitzades les actuacions a realitzar, serà indispensable indicar a l'usuari com finalitzar la sessió i validar que aquesta ha quedat desactivada.

N13. Es mantindrà actualitzat i a disposició de l'Oficina de Seguretat un registre d'usuaris i equips que poden realitzar tasques d'assistència remota, i que es limitaran als mínims necessaris. Així mateix es guardarà registre de les tasques d'assistència portades a terme, on figurarà l'usuari i l'equip que realitza la connexió i la data i hora d'inici i finalització de les tasques. Aquest registre quedarà a disposició de la persona responsable de la contractació del servei, quan aquest estigui subcontractat, i a disposició de l'Oficina de Seguretat i de possibles auditories.

N14. L'accés de tercers[2] per a assistència remota s'ha de fer via VPN.

Transferència remota de fitxers

N15. No es poden fer transferències remotes de fitxers amb *eines o protocols insegurs* a través del nus corporatiu (FTP, *TFTP,* rcp, NetBIOS, etc.). La comunicació es farà sempre de forma xifrada.

Es recomana l'ús de SFTP o SCP per a la transferència segura de fitxers. Es pot consultar un llistat de programaris que ofereixen servei de transferència segura de fitxers en el *Manual d'eines per comunicacions segures en el nus corporatiu de la Generalitat de Catalunya*.

N16. L'accés de tercers per a transferència de fitxers s'ha de fer via VPN.

Publicació a Internet

N17. Tot servei publicat a Internet cal que sigui accedit per nom DNS i no per adreça IP.

Per a serveis publicats únicament en l'àmbit intranet, es recomana igualment que s'hi accedeixi per noms DNS i no per adreça IP.

N18. Només els sistemes frontals (també anomenats "front end") poden ser accedits des d'Internet.

N19. Només es podrà accedir als entorns / aplicacions d'administració des del nus corporatiu i no des d'Internet.

N20. Tot servei publicat a Internet ha d'estar en un equip ubicat en una *DMZ* corporativa o en una DMZ on-site.

N21. Els sistemes frontals tenen sortida directa a Internet. La resta de sistemes, podran tenir connexió cap a Internet sempre i quan es realitzi a través d'un sistema intermediari de control i registre de les connexions.

Accés a serveis corporatius i plataformes departamentals

N22. L'accés o l'intercanvi d'informació amb un sistema d'un altre departament o organisme ha d'estar autoritzat prèviament pel(s) responsable(s) de les dades accedides o intercanviades.

N23. L'accés de tercers[2] a servidors no publicats a Internet només es pot fer via VPN.

N24. Caldrà mantenir un llistat actualitzat dels usuaris autoritzats a accedir als sistemes corporatius.

Gestió de nous projectes

N25. Tot nou projecte que afecti als sistemes o serveis ubicats o accessibles des del nus corporatiu haurà de tenir definida la classificació dels paràmetres de confidencialitat, integritat, disponibilitat i legal segons les directrius marcades per CTTI.

Arquitectura de sistemes

N26. Els diferents entorns d'un sistema (producció, pre-producció, integració, desenvolupament, etc.) han d'estar separats entre si per un tallafocs.

N27. Des d'un entorn de producció, no podrà existir intercanvi d'informació amb entorns de no producció (pre-producció, integració, desenvolupament, etc.).

N28. Tot sistema d'informació ha de tenir una interfície dedicada per a la seva administració i gestió diferent de les productives.

N29. No es podran habilitar serveis d'administració a les interfícies productives *(consulteu l'apartat 2.ÀMBIT I VIGÈNCIA d'aquesta norma).*

N30. Tot sistema d'informació ha de tenir interfície dedicada per la realització de còpies de seguretat diferent de les productives, especialment per a casos de volums de còpies elevats.

N31. Tots els sistemes d'informació han de tenir el rellotge sincronitzat amb els servidors NTP corporatius per garantir la correcta informació de la data i hora en les traces.

N32. Per garantir la disponibilitat i el bon rendiment del servei, el personal de l'àrea TIC i desenvolupadors / tercers subcontractats no podran realitzar la modificació directa de dades en l'entorn de producció. S'estendrà la prohibició als entorns de pre-producció si en l'àmbit existeixen entorns d'integració o desenvolupament.

N33. Per realitzar consultes de lectura no disponibles des de l'aplicació, sobre la base de dades en producció, caldrà cursar petició via SAU per tal que l'administrador de la base de dades de l'aplicació validi i executi la consulta. Aquest control també serà aplicable als entorns de pre-producció si en l'àmbit existeixen entorns de desenvolupament o integració.

Qualsevol excepció a aquest control en **entorns dedicats**, haurà de ser elevada per part del coordinador TIC a l'aprovació conjunta del Director d'Atenció al Client i el Director d'Operacions del CTTI.

N34. La documentació dels sistemes ha d'estar controlada i degudament custodiada.

Gestió del canvi

N35. Qualsevol canvi en els sistemes de seguretat corporatius ha de ser notificat i autoritzat prèviament per l'Oficina de Seguretat.

N36. Existeix un llistat de persones autoritzades a demanar canvis en els sistemes de seguretat (tallafocs, concentradors VPN, etc.). En cas que la petició arribi des d'una bústia de correu genèrica, l'usuari que realitza la petició haurà d'estar clarament identificat.

N37. Tot sistema d'informació ubicat o accessible des del nus corporatiu, previ a la seva posada en producció, haurà de ser analitzat per l'eina de detecció de vulnerabilitats i revisat el compliment de les guies de protecció d'entorns que li apliquin, per part de l'Oficina de Seguretat. Si no compleix els requeriments mínims de seguretat, no serà autoritzada la posada en producció.

Connexió permanent al nus corporatiu de xarxes externes de terceres empreses

N38. Ha d'existir una política de seguretat de la informació en l'empresa contractista. Aquesta política ha d'estar a disposició de l'Oficina de Seguretat per a la seva revisió, així com qualsevol altre registre (normes, procediments, ...) que l'Oficina de Seguretat consideri indispensables per demostrar que l'empresa realitza una bona gestió de la seguretat dels sistemes.

N39. Hi haurà identificat un responsable de seguretat dins l'empresa, que serà l'interlocutor de qualsevol aspecte o incidència relacionat amb la connexió de l'empresa al nus corporatiu. Cal facilitar les seves dades de contacte a l'Oficina de Seguretat.

N40. La gestió d'alta, baixa i modificació de connexions des de l'exterior al nus corporatiu, es realitzarà conforme als procediments especificats en el servei de Connectivitat de terceres empreses (23.0), disponible al catàleg de serveis del CTTI.

N41. S'activaran mecanismes de desconnexió o en el seu defecte de bloqueig de pantalla, a les estacions de treball des de les quals es realitzi la connexió al nus corporatiu, al cap d'un cert temps d'inactivitat (recomanable entre 5 i 10 minuts), de manera que calgui autenticar-se novament per accedir-hi.

N42. El número de màquines de l'empresa externa que es connectaran al nus a través d'un mateix enllaç ha d'estar controlat.

N43. Es mantindrà una llista actualitzada de les persones amb accés a la xarxa corporativa a disposició de l'Oficina de Seguretat.

N44. Existirà un procediment documentat per la gestió dels accessos d'usuaris a la xarxa (altes, baixes, manteniments).

N45.S'haurà de registrar els accessos amb i sense èxit al nus corporatiu.

5. CONTROL

El control del compliment d'aquesta norma es realitzarà mitjançant auditories periòdiques segons s'estableix en el *Pla d'auditories de seguretat*.
En cas de detecció d'incompliment reiterats s'implantaran controls que garanteixin el compliment de la norma.

En el cas que no s'apliqui algun dels controls d'aquesta norma, caldrà justificar i documentar aquestes excepcions. 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

En cas d'incompliment de l'empresa contractista 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

L'àrea de Qualitat, Seguretat i Relacions amb Proveïdors del CTTI publicarà aquesta norma al repositori d'estàndards de la intranet del CTTI.

8. REVISIÓ

Aquesta norma es revisarà anualment.

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

9. GLOSSARI DE TERMES

DMZ: De l'anglès DeMilitarized Zone (Zona Desmilitaritzada), fa referència a una subxarxa aïllada de la resta mitjançant elements de filtratge amb accessos limitats tant d'entrada com de sortida per motius de seguretat.

Eines o protocols insegurs: Totes aquelles utilitats i comunicacions que no garanteixin la confidencialitat de les dades que es transmeten. En particular, tots els protocols que requereixen autenticació (usuari i contrasenya), si aquesta s'envia en text clar, o tots els intercanvis d'informació en què les dades no viatgen xifrades.

Hardening: S'entén com el procés de securització i protecció dels sistemes d'informació. La finalitat és fer més robustos els sistemes en front d'atacs i incidents de seguretat.

ICMP: *Internet Control Message Protocol*. Protocol d'intercanvi de missatges entre equips, utilitzat, entre altres, per la utilitat ping.

Serveis TIC Centrals: Serveis TIC Centrals de Caràcter Continuat de la Generalitat de Catalunya, gestionats pel Centre de Telecomunicacions i Tecnologies de la Informació (CTTI).

TELNET: Protocol que proporciona l'habilitat d'executar comandes d'usuari en un equip de forma remota. Aquest protocol és insegur degut a que envia tant l'autentificació de l'usuari com les comandes en text pla per la xarxa.

TFTP: *Trivial File Transfer Protocol*. Utilitat de transferència de fitxers semblant al FTP però més senzilla, tot i que igualment insegura.

10. DOCUMENTACIÓ REFERENCIADA

- GE-GUI20 Norma de gestió de comptes administració sistemes
- GE-GUI19 Norma de contrasenyes
- SC-NOR02 Norma de connexió d'equips de tercers
- GE-PRO01 Procediment de notificació d'incidents de seguretat
- GE-MAN01 Manual d'eines per comunicacions segures en el nus corporatiu de la Generalitat
- PLA-GSEG-070328 Pla d'auditories de seguretat
- PRO-GSEG-080922 Procediment d'alta d'equipaments al Nus
- PRO-GSEG-080311 Procediment de gestió excepcions estàndards seguretat

NOTA: Consultar els documents en la seva última versió.

11. PARAULES CLAU

Protocols, xifrar, administració, transferència de fitxers, accés remot, consola remota, comunicació, nus corporatiu, seguretat

12. HISTÒRIC DEL DOCUMENT

Versió 1.0
Versió inicial

Versió 2.0
Conversió de guia a norma d'àmbit Generalitat. Per a més informació, consultar la fitxa de l'estàndard.