ÍNDEX

Versió	Redactat / revisat per	Aprovat per	Data aprovació	Data publicació
1.0.	CTTI – Qualitat i Seguretat	Comitè de Direcció del CTTI	26/9/2006	28/9/2006
2.0.	CTTI, Oficina Seguretat, lots	CTTI – QSRaP	25/2/2009	9/3/2009

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

RESUM

OBJECTIU

L'objectiu d'aquesta guia és el de proporcionar uns controls de seguretat a implantar en la configuració i explotació dels sistemes tallafocs, així com contemplar les tasques pròpies d'administració d'aquests sistemes i la gestió del canvi en els mateixos.

ÀMBIT

Aquesta guia va destinada als administradors i responsables de planificació, manteniment i explotació dels sistemes tallafocs (sistemes de filtratge de paquets) ubicats dins del nus corporatiu de la Generalitat de Catalunya.

1 OBJECTIU

Els tallafocs són els elements que protegeixen els serveis de xarxa entre els diferents segments que la composen. La seva finalitat és la de restringir l'ús de sistemes a les adreces IP que estan autoritzades a fer-ho, i impedir-ho a la resta, a la vegada que formen murs de contenció en casos d'intrusió als sistemes de la xarxa. Són, per tant, els elements principals en la seguretat perimetral i interna de la xarxa. Es requereix així que aquests sistemes es configurin i s'operin seguint uns criteris de seguretat que garanteixin la integritat, confidencialitat i disponibilitat de la informació i dels serveis que protegeixen.

L'objectiu d'aquesta guia és el de proporcionar uns controls de seguretat a implantar en la configuració i explotació dels sistemes tallafocs, així com contemplar les tasques pròpies d'administració d'aquests sistemes i la gestió del canvi en els mateixos.

2 ÀMBIT I VIGÈNCIA

Aquesta guia va destinada als administradors i responsables de planificació, manteniment i explotació dels sistemes tallafocs (sistemes de filtratge de paquets) ubicats dins del nus corporatiu de la Generalitat de Catalunya.

Entrarà en vigor el dia 1/3/2009.

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

És d'obligat compliment en l'àmbit dels Serveis TIC Centrals de Caràcter Continuat de la Generalitat de Catalunya gestionats pel CTTI (d'ara endavant "*Serveis TIC Centrals*"), a excepció del control C15 mentre no estigui definida la forma d'implantació d'aquest control.

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:

- 6.1.3 Assignació de les responsabilitats en la Seguretat de la Informació
- 6.2.3 Requeriments de seguretat en els acords amb les terceres parts
- 10.1.2 Gestió dels canvis
- 10.1.3 Segregació de funcions
- 10.2.1 Prestació del servei
- 10.5.1 Còpies de seguretat de la informació
- 10.6.1 Controls de xarxa
- 10.6.2 Seguretat dels serveis de xarxa
- 10.10.1 Registres d'auditoria (logging)
- 10.10.4 Registres d'administradors i operadors
- 10.10.6 Sincronització de rellotges
- 11.4.1 Política d'ús dels serveis de xarxa
- 11.4.6 Control de connexió a la xarxa
- 11.5.1 Processos de connexió segurs
- 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 controls de seguretat orientats a garantir la confidencialitat, privacitat, integritat i disponibilitat de la informació dels sistemes protegits per aquests tallafocs. Sota la columna "categoria", s'especifiquen els aspectes de seguretat que cada control reforça (confidencialitat– C, integritat– I, disponibilitat– D).

4.1. IN- Instal·lació i manteniment

OBJECTIUS	
Definir els controls a tenir en compte a l'hora d'instal·lar un nou sistema tallafocs i el seu posterior manteniment.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C1. La instal·lació d'un nou sistema tallafocs haurà de ser autoritzada per l'Oficina de Seguretat.	C I D
C2. Quan es tracti d'una migració d'un tallafocs anterior i calgui transferir les regles de l'un a l'altre, caldrà validar que aquestes donen compliment als estàndards de seguretat.	I
C3. Cal mantenir els sistemes de tallafocs amb les últimes versions que solucionin vulnerabilitats de seguretat detectades.	C I D
C4. La desconnexió o baixa d'un sistema de tallafocs, haurà de ser notificat a l'Oficina de Seguretat en la major brevetat possible per a poder analitzar l'impacte derivat de l'actuació.	C I D

4.2. CN – Configuració

Aquests controls en la configuració dels sistemes tallafocs 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 Configuració general dels equips

OBJECTIUS	
Configuració del sistemes tallafocs.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C5. Si els equips tallafocs no tenen una consola de gestió, tindran una interfície dedicada per a la seva administració diferent de les productives.	I D
C6. Si es disposa de consola de gestió, aquesta es col·locarà en una xarxa separada de la de l'equip tallafocs que la consola administra. NOTA: Pel cas dels tallafocs virtuals Cisco de l'àmbit dels Serveis TIC Centrals, aquest control no és d'aplicació, ja que es gestionen a través de la interfície virtual securitzada pel propi tallafocs virtual.	I D
C7. Els rellotges dels sistemes tallafocs s'hauran de mantenir sincronitzats mitjançant el protocol *NTP* amb els servidors de temps corporatius per garantir el no repudi de les traces que es generen en cas d'anàlisi d'un incident.	I
C8. No estarà permès l'accés per protocols insegurs als sistemes des de qualsevol origen. Es podran utilitzar protocols estàndard (*HTTPS*, *SSH*, etc.) o propietaris de sistemes que garanteixin que la comunicació sigui xifrada.	C
C9. Caldrà fer còpies de seguretat de les configuracions dels equips tallafocs amb una periodicitat mínima d'una setmana.	D

4.2.2 Configuració de regles de filtratge

OBJECTIUS	
Configuració de les regles associades als tallafocs.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C10.Les regles de nova creació o que es modifiquin, caldrà que donin compliment als	I D

estàndards de seguretat del CTTI. En cas de no ser així, l'Oficina de Seguretat tramitarà una excepció de seguretat.	
C11. La sol·licitud de llistats de regles de tallafocs caldrà que sigui cursada pel responsable de l'àmbit o servei a través dels canals establerts (SAU CTTI).	C
C12. A cada regla de tallafocs s'hi haurà d'adjuntar en el camp de comentari el número de la petició al SAU. Si degut a una situació d'urgència no existeix número de tiquet, caldrà informar la data d'execució de la regla i el nom de l'autoritzador.	I
C13. En cas que es modifiqui el contingut d'una regla (implícita o explícitament), s'haurà d'adjuntar en el camp de comentari la mateixa informació mínima (C12), tot conservant els comentaris anteriors.	I
C14. En el cas que es desactivi temporalment part o la totalitat d'una regla, s'haurà d'adjuntar en el camp de comentari la mateixa informació mínima (C12), tot conservant els comentaris anteriors.	I
C15. Es tindrà especial cura en respectar el temps de vida de les regles aprovades. Quan el sistema tallafocs ho permeti s'haurà de posar la data de caducitat de la regla per a la desactivació automàtica. Si no ho permet, s'hauran d'inhabilitar manualment les regles caducades. En aquest cas s'haurà d'establir un mecanisme de control per a marcar la caducitat de la regla, com ara la data de caducitat en el camp de comentari.	I D
C16. La creació d'un nou tallafocs al Nus Corporatiu implicarà crear les regles d'accés dels equips d'auditoria de l'Oficina de Seguretat a totes les xarxes que protegeix el tallafocs.	C

4.3. IA – Identificació i Autenticació

OBJECTIUS	
Identificar i autenticar correctament als usuaris que requereixen accedir als sistemes tallafocs.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C17. S'utilitzarà un nom d'usuari únic i inequívoc per a cada persona que requereixi accedir als sistemes tallafocs. Aquest ID serà per a ús personal i exclusiu de la persona a qui s'assigni. Aquesta regla pot no aplicar als usuaris de només lectura.	C
C18. No s'activarà en cap cas cap sistema de recordatori de ID i/o contrasenya.	C

4.4. CA – Control d'accés

OBJECTIUS	
Controlar l'accés dels usuaris als sistemes tallafocs.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C19. Es limitarà l'accés als sistemes tallafocs només a aquells usuaris que ho requereixin per tasques d'administració, operació, revisió i/o auditoria. Caldrà mantenir una llista actualitzada d'usuaris autoritzats, que haurà d'estar a disposició de l'Oficina de Seguretat.	C
C20. La creació d'un nou tallafocs departamental implicarà crear un usuari de consulta pel gestor tecnològic de l'àmbit.	C
C21. La creació d'un nou tallafocs implicarà crear els usuaris amb finalitats d'auditoria per a l'Oficina de Seguretat.	C
C22. La creació de nous usuaris o modificacions dels existents amb accés als sistemes tallafocs per a tasques de revisió i/o auditoria haurà d'estar autoritzada per l'Oficina de Seguretat.	C I
C23. Caldrà disposar d'un procediment d'altes, baixes i modificacions dels usuaris amb accés als tallafocs que contempli els requeriments especificats en aquesta guia.	C I
C24. Es complirà la *Norma de gestió de comptes d'administrador de sistemes* per a garantir el control dels comptes amb privilegis d'administració sobre els tallafocs.	C

4.5. MN – Monitoratge

OBJECTIUS	
Registrar totes les accions en els sistemes per tal de poder conduir futures investigacions en cas de necessitat i atribuir-ne responsabilitats.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C25. S'habilitaran les traces en els sistemes tallafocs que garanteixin l'estudi d'incidències o de funcionaments anòmals.	C I
C26. Per als sistemes tallafocs crítics es disposarà d'alertes que s'activaran en cas de funcionament anòmal o caiguda del servei.	C I D
C27. Es registraran els accessos amb i sense èxit d'usuaris als sistemes tallafoc. Aquestes traces les haurà de revisar mensualment el responsable del servei de xarxa del nus corporatiu.	I D
C28. 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

4.6. AU – Auditoria

OBJECTIUS	
Controlar la configuració dels diferents sistemes i facilitar les traces del sistema a l'eina centralitzada de gestió de traces.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C29. Caldrà guardar les traces durant un període mínim de 90 dies. Així mateix caldrà donar compliment a la Norma de gestió de traces[1], on es recullen amb detall els requeriments per a la gestió de les traces.	I D
C30. Caldrà proporcionar les traces per l'estudi d'incidències o funcionaments anòmals a petició de la Oficina de Seguretat. El temps d'entrega de les traces ha de ser menor a l'indicat en els *Acords de Nivell de Servei* (ANS) establerts en els contractes.	I D

4.7. DI – Divulgació

OBJECTIUS	
Formació i conscienciació als administradors i operadors de sistemes tallafocs de la importància d'implantar mesures de seguretat en aquests sistemes.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C31. Revisar les notificacions de seguretat que l'Oficina de Seguretat elabora on es recullen les vulnerabilitats detectades per a diferents sistemes.	C I D

4.8. 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 sistemes tallafocs.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C32. Es recollirà contractualment el compliment de les normes i guies que el CTTI tingui per equips tallafocs així com qualsevol altra norma de gestió o administració que sigui d'aplicació.	C I D
C33. Es garantirà el compliment de la *Norma de contractació de Tercers*.	C I D

[1] Actualment en revisió.

C34. Es garantirà 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 d'entrega de traces a l'Oficina de seguretat (C28). • Temps de resposta per canvis / noves instal·lacions. • Compliment i actualització dels controls de seguretat. • Gestió de problemes. • Etc. L'incompliment d'acords de nivell de servei haurà de comportar penalitzacions econòmiques al proveïdor.	C I D
C35. Es recollirà contractualment les següents obligacions per part del proveïdor: • Pla de recuperació en cas de desastre. • Mesures de seguretat física pels equips externalitzats. • Dret d'auditar al proveïdor per part del CTTI, l'Oficina de Seguretat o les persones per aquesta designades.	C I D

5 CONTROL

Per a l'àmbit dels *Serveis TIC Centrals* 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 que no s'apliqui algun dels controls d'aquesta guia, caldrà justificar i documentar aquestes excepcions. Per a l'àmbit dels *Serveis TIC Centrals*, 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

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

8 REVISIÓ

Aquesta guia ha de ser revisada 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

HTTP: *Hypertext Transfer Protocol*. Protocol d'aplicació per a la transmissió de continguts web.

HTTPS: *HTTP over SSL*. Protocol d'aplicació web segura que xifra la comunicació entre el navegador i el servidor web.

NTP: *Network Time Protocol*. Protocol utilitzat per a sincronitzar els rellotges dels equips en una xarxa.

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).

SSH: *Secure Shell*. Programari que permet establir una sessió amb un equip remot i administrar-lo mitjançant una línia de comandes. Xifra la comunicació entre el client i el servidor per evitar que sigui desxifrada si s'intercepta.

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 texte pla per la xarxa.

10 DOCUMENTACIÓ REFERENCIADA

- SC-NOR07 Norma de gestió de comptes administrador sistemes
- SC-NORxx Norma de gestió de traces
- CT-NOR03 Norma de contractació de tercers
- GE-PRO01 Procediment de notificació d'incidents de seguretat
- PLA-GSEG-070328-v2.0-Pla d'auditories de seguretat

Consulteu aquests documents de referència en la seva última versió.

11 PARAULES CLAU

Tallafocs, filtratge, regla, auditoria, administració, controls de seguretat, firewall.

12 HISTÒRIC DEL DOCUMENT

Versió 1.0

Versió inicial.

Versió 2.0 – 25/3/2009

Versió revisada de l'estàndard. Veure la fitxa de l'estàndard per a més informació.