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
2.0	CTTI – QSRaP	CTTI – QSRaP	20/4/2009	18/5/2009

Estàndard signat digitalment pel:
Generalitat de Catalunya
Centre de Telecomunicacions i Tecnologies de la Informacio
Estàndard aprovat
Barcelona
2009.05.18 10:11:59 +02'00'

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

RESUM

1. Objectiu: Definir els controls per administrar i gestionar la seguretat en els equips amb sistemes operatius Solaris.

2. Àmbit: Aquesta guia va destinada als administradors i responsables de manteniment dels equips Solaris de la Generalitat de Catalunya.

A més d'aquesta guia, s'hauria de complir allò que estigui establert a qualsevol altra guia d'administració de sistemes en general i de Solaris en particular, ja que en aquesta guia s'identifiquen els controls específics per garantir un mínim de seguretat en els equips amb sistema operatiu Solaris.

3. Descripció:

Es presenten a continuació els controls de seguretat orientats a garantir la confidencialitat, privacitat, integritat i disponibilitat de la informació de sistemes basats en Solaris.

Aquests s'agrupen per grups d'accions o procediments operatius orientats a combatre les amenaces a les quals un equip pot estar exposat. L'aplicació dels controls d'una manera lògica, ordenada i planificada reduirà progressivament les vulnerabilitats del sistema i, per tant, l'exposició als riscos.

1 OBJECTIU

Definir els controls per administrar i gestionar la seguretat en els equips amb sistemes operatius *Solaris*.

2 ÀMBIT I VIGÈNCIA

Aquesta guia va destinada als administradors i responsables de manteniment dels equips *Solaris* 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.

A més d'aquesta guia, s'hauria de complir allò que estigui establert a qualsevol altra guia d'administració de sistemes en general i de *Solaris* en particular, ja que en aquesta guia s'identifiquen els controls específics per garantir un mínim de seguretat en els equips amb sistema operatiu *Solaris*, però no per administrar el sistema en sí. Així mateix, s'han de tenir en compte les recomanacions del fabricant, Sun Microsystems.

És d'obligat compliment en l'àmbit dels *Serveis TIC Centrals*.

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

Entrarà en vigor el dia 18 de maig de 2009.

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 27002:2005:

- 6.2.3 Requeriments de seguretat en els acords amb les terceres parts
- 10.10.1 Registres d'auditoria (logging)
- 10.10.6 Sincronització de rellotges
- 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
- 12.5.3 Restriccions en els canvis als paquets de programari
- 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 de sistemes basats en Solaris.

Aquests s'agrupen per grups d'accions o procediments operatius orientats a combatre les amenaces a les quals un equip pot estar exposat. L'aplicació dels controls d'una manera lògica, ordenada i planificada reduirà progressivament les vulnerabilitats del sistema i, per tant, l'exposició als riscos.

Cal remarcar que les configuracions de seguretat indicades en aquesta guia, caldrà provar-les en un entorn de proves abans d'aplicar-les en servidors que estiguin en explotació.

3.1. IN - Instal·lació i manteniment

OBJECTIUS	
Identificar les mesures de seguretat a tenir en compte durant el procés d'instal·lació del sistema operatiu *Solaris*, així com les tasques a enllestir periòdicament per tal de fer més segur el sistema.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C1. Durant la instal·lació inicial del sistema, crear les particions de manera que les dades d'usuaris, el programari que s'instal·larà i el propi sistema operatiu estiguin separats i	D

no s'afectin mútuament. Sobretot cal protegir la partició amb el sistema operatiu i els seus fitxers temporals.	
C2. Mantenir el sistema actualitzat amb els pegats de seguretat i els paquets de programari adequats. Pels sistemes ubicats en l'àmbit dels Serveis TIC Centrals, cal donar compliment a la *Norma de gestió de vulnerabilitats de programari base*.	C I D
C3. No instal·lar programari o paquets innecessaris en el sistema.	C I D
C4. No instal·lar programari o paquets de fonts desconegudes o no fiables.	C I D
C5. Sempre que tècnicament sigui possible, instal·lar un programari antivirus i mantenir-lo actualitzat de forma contínua. En cas que el sistema serveixi de passarel·la o d'emmagatzemament de fitxers, el control serà d'obligat compliment.	C I D
C6. S'hauran de sincronitzar els rellotges amb servidors NTP corporatius o servidors NTP corporatius intermedis si existeixen i, en tot cas, mantenir els rellotges dels sistemes en hora.	C I
C7. Netejar els usuaris i grups per defecte que es creen durant la instal·lació. Si no són necessaris pels diferents serveis que s'hagin d'instal·lar, cal eliminar-los o bé inhabilitar-los per evitar forats de seguretat.	C I
C8. Esborrar fitxers associats a un usuari quan aquest sigui eliminat del sistema, ja que sinó queden sense propietari assignat. Per a trobar aquests fitxers, executar la comanda amb permisos d'administrador: find / -nouser –ls	C I
C9. Caldrà donar compliment a la *Norma de còpies de seguretat* per a garantir que es realitza còpia de seguretat dels sistemes.	C I D

Recomanacions

R1. Es recomana crear una partició on residiran els fitxers web. S'indicarà al sistema operatiu que aquesta partició no és executable.
R2. Es recomana que les particions es configurin amb els següents privilegis:
/boot → només lectura
/home → sense permisos d'execucio, nosuid i nodev
/tmp → sense permisos d'execució i nosuid
/dev/shm → nosuid i noexec
R3. No donar servei de xarxa a un equip fins que no hagi acabat la instal·lació inicial del sistema operatiu i no s'hagin aplicat les mesures de seguretat adequades, incloent els pegats de seguretat necessaris.

3.2. CN - Configuració

OBJECTIUS	
Identificar les mesures de seguretat a aplicar després de la instal·lació inicial del sistema o durant la utilització del mateix, per tal de configurar-lo adequadament.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C10. Les contrasenyes s'han de guardar de forma xifrada i s'han de modificar els permisos d'accés al fitxer de contrasenyes per evitar que siguin de lectura per a tots els usuaris.	C I
C11. Cal donar compliment a la *Norma de gestió de comptes d'administració de sistemes* per a garantir la correcta definició i gestió dels comptes amb privilegis d'administració.	C I
C12. Inhabilitar tots aquells serveis que no siguin necessaris o insegurs.	C I D
C13. No configurar el X Server si no és necessari realment en l'entorn.	C I D
C14. Per tal que es registrin els accessos no autoritzats, crear el fitxer /var/adm/loginlog amb permís de lectura i escriptura només per a l'usuari *root*.	C I D
C15. No configurar l'equip per fer encaminament de paquets IP si no es tracta d'un equip encaminador entre dos o més xarxes.	D
C16. No permetre el reenviament de trames o paquets IP entre diferents interfícies de xarxa quan una trama enviada a una interfície vagi dirigida a una altra. Així es	D

reforçarà la seguretat contra atacs de suplantació d'adreça IP i en tot moment es podrà saber d'on provenia una trama, permetent refusar-la en cas necessari.	
C17. Configurar l'entorn de xarxa per tal que no respongui a les peticions de broadcast que no siguin estrictament necessàries per un determinat servei. Així es reduirà el risc d'atacs de denegació de servei.	D
C18. La generació de números de seqüència dels paquets TCP és pseudo-aleatòria per defecte. Així doncs, per augmentar el nivell de seguretat, configurar el paràmetre TCP_STRONG_ISS del fitxer /etc/default/inetinit amb valor 2 per reduir el risc d'atacs de suplantació d'adreça IP.	C D
C19. No incloure en cap cas el directori "." (l'actual sigui quin sigui) en la ruta de recerca o *PATH* per defecte.	C I D
C20. Tots els directoris de la ruta de recerca o *PATH* per defecte de l'usuari *root* han de ser modificables (permís d'escriptura) únicament per l'usuari *root*.	C I D
C21. Deshabilitar l'execució de *shell scripts* com usuari *root* mitjançant *SUID bit*. Utilitzar exclusivament scripts amb els privilegis dels usuaris que els executen, i substituir l'ús del SUID bit per scripts amb privilegis adequats, executats directament per usuaris amb els privilegis necessaris o amb programari d'execució de tasques.	C I D
C22. Afegir una línia "set noexec_user_stack=1" al fitxer /etc/system per tal que el codi d'un usuari no pugui executar-se des de la pila i protegir-se així contra atacs de desbordament de pila.	C I D
C23. Configurar correctament l'aplicatiu sudo garantint que: • No s'habiliten privilegis per tots els usuaris (all). • S'especifiquen línies de comandes o binaris concrets per a què estiguin controlades les accions que es poden executar amb privilegis d'administració.	C I D
C24. Modificar els missatges de benvinguda (login banners) per evitar que es proporcioni informació del sistema. Canviar el tipus de missatge pel següent exemple: "AVÍS ALS USUARIS: L'ús no autoritzat d'aquest sistema no està permès. Les activitats seran registrades."	C I D
C25. Eliminar els fitxers .rhosts i .netrc ja que emmagatzemen les contrasenyes en clar. Cal eliminar també les entrades del fitxer /etc/hosts.equiv. Aquests fitxers defineixen sistemes i usuaris que poden executar comandes de forma remota sense contrasenya.	C I D
C26. En sistemes ubicats en entorns de producció, no hi pot haver compiladors instal·lats.	I D
C27. En sistemes ubicats en entorns de producció, només estaran instal·lats aquells llenguatges interpretats necessaris per a l'execució del servei.	I D
C28. En funcionament, un servei mai no podrà executar-se amb permisos de root.	C I D
C29. Restringir l'accés al directori de logs i els fitxers de syslog als usuaris sense privilegis	C
C30. No habilitar serveis d'administració del sistema a les interfícies de producció. No habilitar serveis d'administració del sistema a les interfícies de producció. Consultar l'apartat 2. ÀMBIT I VIGÈNCIA, de la *Norma de mesures de seguretat en el nus corporatiu TIC de la Generalitat.*	C I D

Recomanacions

R4. Provar les configuracions de seguretat en un entorn de proves abans d'aplicar-les en servidors que estiguin en explotació.
R5. Revisar que existeix una limitació del nombre de processos que un sol usuari pugui tenir actius en la taula de processos.
R6. Revisar que existeix una limitació del nombre total de processos del sistema en la taula de processos, per tal que no hi hagi una sobrecàrrega de recursos que impliqui la caiguda del sistema.
R7. Configurar el muntatge dels sistemes de fitxers per evitar que als que són muntats dinàmicament, com unitats de CDROM i de disc flexible, es puguin executar fitxers amb el *SUID bit* activat. Això es pot aconseguir amb el paràmetre *nosuid*.
R8. Utilitzar les llibreries PAM per a l'autenticació d'usuaris i aplicacions al sistema. Disposen de funcionalitats per a reforçar la robustesa de l'autenticació, gestió de contrasenyes, traçabilitat i gestió de les sessions.

3.3. MN- Monitoratge

OBJECTIUS	
Identificar quines accions i activitats dels usuaris que es realitzen en el sistema cal registrar.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C31. Caldrà donar compliment als requeriments de la *Norma de gestió de traces* per a garantir la traçabilitat i custòdia dels esdeveniments dels sistemes.	C I
C32. Pels sistemes d'àmbit departament / ens, es connectaran a eines de correlació de traces pròpies quan existeixin; de no ser així, caldrà guardar les traces durant un període mínim d'1 any i revisar-les periòdicament per a detectar anomalies o incidències en el funcionament del sistema.	C I
C33. 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

Recomanacions

R9. Es recomana, revisar periòdicament les traces per a detectar activitats anòmales que puguin comprometre la seguretat del sistema

3.4. ID - Intercanvi de dades

OBJECTIUS	
Garantir que l'intercanvi de dades es realitza de forma segura.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C34. No fer servir *NIS* en cap cas, ja que és molt insegur. En cas de necessitat de compartició d'informació, utilitzar *NIS+*, configurant-ho per garantir les oportunes mesures de seguretat amb: • Mecanismes d'autenticació per accedir al servei. • Validació a nivell d'IP dels clients a l'hora de connectar-se amb el servidor. • Mecanismes d'autorització d'accés als objectes *NIS+*, amb els mínims privilegis.	C I
C35. No fer servir NFSv2 en cap cas, ja que és molt insegur. En el seu lloc, utilitzar versions superiors i només si és necessari, habilitant: • Mecanismes d'autenticació per accedir al servei. • Validació a nivell d'IP dels clients a l'hora de connectar-se amb el servidor. • Mecanismes d'autorització d'accés als objectes amb els mínims privilegis.	C I
C36. Exportar remotament directoris a altres equips i muntar directoris exportats per d'altres amb el major nombre de mesures de seguretat possible i amb els mínims permisos d'accés per usuaris remots. S'hauria de tenir en compte que: • Sempre que sigui possible, cal exportar indicant l'opció *secure* per cada directori. • No exportar ni muntar amb permisos d'escriptura si no és necessari. • Exportar directoris donant accés a una llista acotada de sistemes remots. • Exportar amb les opcions *nosuid* i *noexec*, si s'escau. • Per tal que el *root* no sigui permisos d'administració al sistema remot (on es muntarà el directori o sistema de fitxers), exportar amb l'opció *root_squash*.	C I

3.5. CA - Control d'accés

OBJECTIUS	
Proveir als usuaris i grups de privilegis o drets d'accés als sistemes *Solaris*.	
CARACTERÍSTIQUES	
Descripció	**Categoria**

C37. No es podra accedir com usuari root. S'han d'utilitzar usuaris nominals per cada administrador.	C I D
C38. Limitar l'accés als serveis del sistema que no siguin publicats per a tots els usuaris. Poden utilitzar-se mecanismes com iptables o TCP_wrappers.	C I
C39. No utilitzar aplicacions de connexió remota en les quals la contrasenya viatgi en clar per la xarxa, com per exemple telnet, rlogin, rsh i rexec. Utilitzar les protocols segurs com sftp, scp o ssh.	C I D
C40. Fer un ús adequat dels usuaris, grups, propietat dels fitxers i permisos dels usuaris i grups sobre els fitxers per tal de mantenir la confidencialitat i integritat de les dades que continguin aquests fitxers. Sempre caldrà garantir el principi de mínims privilegis.	C I
C41. Inhabilitar l'accés al compte d'invitat.	C I D

3.6. AU - Auditoria

OBJECTIUS	
Recollir les tasques i activitats d'auditoria dels sistemes.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C42. Caldrà facilitar les tasques d'auditoria per part de l'Oficina de Seguretat davant la revisió del compliment dels requeriments de seguretat marcats pel CTTI.	C I D

3.7. 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 de l'administració de sistemes *Solaris*.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C43. Es recollirà contractualment el compliment de les normes i guies que el CTTI tingui per l'entorn *Solaris* així com qualsevol altra norma de gestió o administració que sigui d'aplicació.	C I D
C44. Es garantirà el compliment de la *Norma de contractació de tercers*.	C I D
C45. 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 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

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 de què 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 Relació 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

NIS: Network Information System, és un sistema d'informació compartida entre tots els equips d'una xarxa que estiguin al mateix domini. Entre aquesta informació compartida estan les dades de les comptes d'usuari, inclosa la contrasenya, amb lo qual el risc d'atac per força bruta augmenta.

NIS+: versió de NIS millorada per fer més segur el seu ús, entre d'altres millores.

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

Patchdiag: Eina incorporada a Solaris per verificar els pegats d'un sistema i comparar-los amb la llista de recomanats i de crítics que ofereix Sun. Per utilitzar aquesta eina cal un contracte de manteniment amb Sun Microsystems.

PATH: Variable d'entorn exclusiva de cada usuari, que la pot personalitzar, i que serveix per buscar una comanda escrita a la línia de comandes en una sèrie de directoris, per no haver d'escriure cada vegada la ruta completa d'aquesta comanda.

Root: Usuari administrador del sistema en equips amb sistema operatiu Linux (i d'altres basats en Unix); té l'UID o identificador d'usuari 0.

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).

Shell scripts: Fitxers de text que contenen un conjunt de comandes a executar per lots.

SfpDB: Solaris Fingerprint Database, és un servei gratuït de Sun Microsystems per comparar fitxers del sistema amb una base de dades oficial i poder esbrinar si un fitxer ha estat modificat.

Solaris: Sistema operatiu multiusuari i multitarea propietat de Sun Microsystems que permet que un equip doni diferents tipus de servei als usuaris del sistema. Inicialment va ser concebut com sistema operatiu per equips amb processador Sparc, però actualment hi ha versions per estació de treball i servidors amb arquitectura x86.

Sudo: Paquet de programari que permet l'execució d'un programa binari o d'un shell script com un usuari diferent. El root ha de configurar aquest paquet per tal d'identificar quin usuari pot executar què programa binari o shell script com quin altre usuari.

SUID bit: Permís especial dels fitxers per executar-los amb un UID o identificador d'usuari diferent del que escriu la comanda des de la línia de comandes.

TCP_wrappers: és una utilitat afegida a algunes versions de Solaris que permet indicar quins equips remots poden i quins no poden utilitzar determinats serveis. Així doncs, és una etapa més en la millora de la seguretat d'un sistema.

10 DOCUMENTACIÓ REFERENCIADA

- NOR-GSEG-070308-v1.0 Norma de gestió de vulnerabilitats de programari base
- GE-GUI20 Guia de gestió de comptes administració sistemes
- GE-GUI40 Guia de copies de seguretat
- GE-PRO01-01 Procediment de Notificació d'Incidents de Seguretat
- SC-NOR16-01 Norma de gestió de traces
- GE-NOR28 Norma de mesures de seguretat en el nus corporatiu TIC de la Generalitat.

Consulteu aquests documents de referència en la seva última versió

- Documentació:
  - Pegats de seguretat (http://sunsolve.sun.com)
  - Blueprints (http://www.sun.com/blueprints)
  - CERT (http://www.cert.org/security-improvement/implementations/i012.01.html)
  - Seguretat en Solaris (http://www.kernelthread.com/publications/security/solaris.html)
  - Red Iris (http://www.rediris.es/cert/doc/unixsec/node16.html)

Eines
- De propòsit general:
  - JASS o JumpStart Architecture and Security Scripts, paquet d'eines també conegut com Solaris Security Toolkit (integrat amb Solaris)
  - Titan (http://www.fish.com/titan/TITAN_documentation.html)
- Per comprovar o mantenir la integritat dels fitxers de sistema:
  - Tripwire (http://www.tripwire.org)
  - ASET o Automated Security Enhancement Tool (integrat amb Solaris)
  - SfpDB o Solaris Fingerprint Database (integrat amb Solaris)
  - SfpC o Solaris Fingerprint Database Companion (integrat amb Solaris)
  - SfpS o Solaris Fingerprint Database Sidekick (integrat amb Solaris)
  - BART o Basic Audit Reporting Tool (integrat amb Solaris)
- Per xifrar dades, fitxers i comunicacions:
  - OpenSSH (integrat a Solaris 9, també disponible a http://www.openssh.net)
  - MD5 (http://ftp.cerias.purdue.edu/pub/tools/unix/cerias/md5)
- Autenticació segura:
  - PAM o Pluggable Authentication Modules (integrat amb Solaris) (http://www.kernel.org/pub/linux/libs/pam/index.html)
  - Kerberos (http://nii.isi.edu/info/kerberos/)
  - TCP wrappers (integrat amb Solaris 9 al paquet SFWtcpd, disponible per versions anteriors a http://www.sunfreeware.com)
- Administració d'usuaris, grups i rols:
  - RBAC o Role Based Access-Control (integrat amb Solaris)
  - Epasswd (http://www.nas.nasa.gov/Groups/Security/epasswd/)
  - Npasswd (http://www.utexas.edu/cc/unix/software/npasswd/)
- Gestió de registres del sistema
  - BSM o Basic Security Module (integrat amb Solaris)
  - LogSurfer (ftp://ftp.cert.dfn.de/pub/tools/audit/logsurfer/)

11 PARAULES CLAU

Sistema operatiu, paquet de programari, administració, usuaris, grups, permisos, pegat de seguretat, particions, línia de comandes, programa binari, solaris, hardenning, protecció

12 HISTÒRIC DEL DOCUMENT

Versió 1.0
Versió inicial.
Versió 2.0
Versió revisada de l'estàndard. Veure la fitxa de l'estàndard per a més informació.