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	5/10/2009	6/10/2009

Estàndard signat digitalment pel:
Generalitat de Catalunya
Centre de Telecomunicacions i Tecnologies de la Informacio
Estàndard aprovat
Barcelona
2009.10.06 12:13:31 +02'00'

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

RESUM

OBJECTIU

Definir els controls a aplicar per a la protecció d'instal·lacions del servidor web *Apache*, amb l'objectiu de garantir la confidencialitat, integritat i disponibilitat de la informació i serveis suportats per aquesta plataforma.

ÀMBIT

Servidors web *Apache* de la Generalitat de Catalunya.

DESCRIPCIÓ

Es recullen els controls de seguretat orientats a garantir la confidencialitat, privacitat, integritat i disponibilitat de la informació de sistemes basat en Servidors web *Apache*.

1 OBJECTIU

Definir els controls per a instal·lar, configurar i mantenir el servidor web *Apache* d'una manera segura, que garanteixi la confidencialitat, integritat i disponibilitat dels serveis web de la Generalitat de Catalunya. Es tracta d'evitar que usuaris malintencionats puguin causar la interrupció del servei web, provocant un deteriorament en la imatge dels organismes i departaments de la Generalitat de Catalunya.

2 ÀMBIT I VIGÈNCIA

Aquesta guia va destinada als administradors i responsables d'instal·lació i manteniment dels servidors web *Apache* de la Generalitat de Catalunya.

L'àmbit d'aquesta guia se cenyeix als entorns d'explotació de serveis web amb *Apache*. No afecta a entorns de proves o integració, ja que moltes de les configuracions poden estar habilitades per qüestions de proves o desenvolupament.

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

La versió actual entrarà en vigor el dia 6 d'octubre 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
- 9.2.1 Ubicació i protecció dels equips
- 10.10.1 Registres d'auditoria (logging)
- 11.4.4 Protecció dels ports de configuració i diagnòstic remot
- 11.5.1 Processos de connexió segurs
- 11.6.1 Restricció d'accés a la informació
- 11.6.2 Aïllament de sistemes sensibles
- 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 en els servidors web *Apache*. Sota la columna "categoria", s'especifiquen els aspectes de seguretat que cada control reforça (confidencialitat– C, integritat– I, disponibilitat– D).

En els diferents controls es parla de les *directives*. Així es com es coneixen els diferents paràmetres de configuració del servidor web, que resideixen en el fitxer de configuració *httpd.conf* i altres fitxers que utilitza *Apache* per a mantenir la configuració.

En aquesta guia es comenten les directives que afecten a qüestions de seguretat del servidor web Apache. Per a obtenir informació detallada de totes les directives, consultar la documentació del servidor web disponible a Internet (veure l'adreça web en el punt *9. Documentació referenciada*).

Les referències a directoris estan realitzades sobre sistemes *Linux*, ja que és normalment l'entorn sobre el que s'instal·la el servidor *Apache*.

4.1. IN - Instal·lació i manteniment

OBJECTIUS	
Requisits en la instal·lació i manteniment del servidor *Apache*.	
CARACTERÍSTIQUES	
Descripció	**Categoria**

C1. Quan calgui instal·lar un nou servidor *Apache*, utilitzar l'ultima distribució estable.	I D
C2. Instal·lar els servidors web Apache en màquines dedicades.	I D
C3. No fer instal·lacions del servidor web Apache en controladors de domini.	I D
C4. Protegir el sistema operatiu, controlant els serveis de xarxa que té habilitats. Cal mantenir el sistema operatiu al dia dels pegats de seguretat. (Veure *Guia protecció entorns Linux, Guia protecció entorns HP-UX, Guia protecció entorns AIX, Guia protecció entorns Solaris, Guia protecció entorns Windows 2003*).	C I D
C5. No donar accés públic al servidor fins que es trobi convenientment protegit.	C I D
C6. El servidor *Apache* cal mantenir-lo actualitzat amb les últimes versions que solucionin vulnerabilitats de seguretat detectades. 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
C7. Validar que el servidor no tingui ja instal·lat per defecte un servidor web Apache. Si és així, cal comprovar que la versió instal·lada no presenta vulnerabilitats de seguretat. És aconsellable realitzar una actualització a la última distribució estable.	I
C8. Instal·lar els mòduls d'Apache estrictament necessaris.	D
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. Si existeixen versions 1.3 d'*Apache* en explotació, és necessari planificar la migració a la versió 2.0 com a mínim, essent recomanable la migració a la versió 2.2.

4.2. CN - Configuració

OBJECTIUS	
Configurar la instal·lació dels servidor web *Apache* per a garantir la seguretat del servei.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C10. Els directoris *bin*, *conf*, *logs* només tindran privilegis d'escriptura de l'usuari *root*.	I
C11. L'executable *httpd* i el directori especificat en la directiva *ServerRoot* només han de tenir privilegis d'escriptura per l'usuari *root* (o l'usuari que executa *Apache*)	I
C12. Quan el servei d'*Apache* s'inicia, ho fa amb l'usuari *root*, ja que només aquest usuari pot activar el port 80 (web). Una vegada arrancat transfereix el control a l'usuari que estigui definit en la directiva *User* que és l'utilitzat per a servir el contingut web. Per això, cal definir un usuari en el sistema per indicar a la directiva *User* que: • No tingui privilegis d'administració • No tingui accés a cap tipus de consola del sistema • No tingui definit el *home*. Mai es posarà *root* com a *User*. Tampoc és recomanable utilitzar l'usuari *nobody* ja que pot tenir altres usos en el sistema. És aconsellable utilitzar un usuari específic com per exemple *apache*.	C I D
C13. No es permet l'ús de *SSI*, degut als problemes de seguretat que presenten.	I D
C14. Evitar executar els *scripts CGI* en qualsevol directori. Limitar en quins directoris es podran executar i controlar l'accés dels usuaris a aquests directoris.	C I D
C15. Revisar que no existeixin *CGI*s per defecte, que poden contenir vulnerabilitats.	I D
C16. La directiva *ScriptInterpreterSource* s'utilitza per indicar quin intèrpret s'utilitzarà per la execució dels *scripts CGI* dels directoris indicats per la directiva *ScriptAlias* (El servidor web intentarà executar tots els fitxers continguts en el directori ja que el marca com a directori d'execució de *CGI*s). Per entorns *Windows*, no utilitzar l'opció *Registry*, ja que implica que es busqui en el registre quin programa es farà servir per a interpretar cada petició. Per tant, cada petició de fitxer *.html* sobre el directori farà que s'obri una instància del *Microsoft Internet Explorer* en el servidor. Això pot provocar que el servidor deixi de funcionar en un període curt de temps.	I D

C17. Controlar els *scripts* d'altres eines incloses en el servidor com pot ser *PHP*, *Perl*, etc. ja que l'usuari amb drets d'execució sobre el servidor web ha de tenir accés sobre aquestes aplicacions.	I D

C18. No permetre l'accés al sistema de fitxers per defecte. Només permetre l'accés als directoris que s'especifiqui concretament. La següent configuració inhabilita l'accés al sistema de fitxers:
`<Directory />`
`Order Deny,Allow`
`Deny from all`
`</Directory>`
	C I D

C19. La directiva *Options* indica quines accions es poden realitzar en un directori. Per defecte, la directiva *Options* permet l'execució de totes les accions i no és recomanable que estigui configurat així. Utilitzar la opció *None* per deshabilitar-ho, o en tot cas, indicar quines opcions estaran activades explícitament. Una de les accions a evitar es la de llistar el contingut dels directoris `Options Indexes` si no existeix cap fitxer *html* per defecte especificat mitjançant la directiva *DirectoryIndex*.	C I D
C20. Configurar una adreça de correu vàlida de l'administrador del servidor web mitjançant la directiva *ServerAdmin*.	D
C21. Configurar el nom del servidor web i el port per on escolta (normalment port 80) mitjançant la directiva *ServerName*.	D
C22. Indicar el directori on està instal·lat *Apache* mitjançant la directiva *ServerRoot*.	D
C23. Cal inhabilitar les pàgines de diagnòstic i manuals d'ajuda instal·lats per defecte.	I D

C24. S'evitarà l'ús dels fitxers de configuració per directoris *.htaccess*. En el seu lloc, incloure les configuracions en el fitxer *httpd.conf*, mitjançant la directiva *Directory*. El fet de tenir diferents fitxers de configuració repartits, pot provocar problemes de seguretat. La següent directiva inhabilita l'ús dels fitxers *.htaccess*:
`<Directory />`
`AllowOverride None`
`</Directory>`
En cas de què s'utilitzessin fitxers de configuració, evitar que se serveixin als clients mitjançant la següent directiva:
`<Files ~ "^\.ht" />`
`Order Allow,Deny`
`Deny from all`
`Satisfy All`
`</Files>`
	I D

C25. Evitar que el servidor web serveixi fitxers de configuració (.bak, .cfg, etc.)	C I D
C26. Si el servidor web ha de servir pàgines personals (directoris on cada usuari pot crear la seva pàgina personal), evitar que es puguin executar *SSI*, *CGI* o qualsevol altre utilitat que podria comprometre la seguretat del sistema. Fins a la versió 2.1.4 ve habilitat per defecte les pàgines personals. Si no s'utilitzen cal desactivar-ho explícitament. És molt important que si estan actius els directoris personals, s'inclogui la directiva que inhabilita aquesta funcionalitat per l'usuari *root*: `UserDir disabled root`	C I D

C27. Modificar les pàgines d'error perquè en cas de mostrar un error no informi de la versió del servidor. En el seu lloc, mostrar informació de l'error maquetada amb la fulla d'estil del lloc web, enlloc del missatge d'error que retorna directament el servidor. La configuració es realitza mitjançant la directiva *ErrorDocument*.
NOTA: Si s'usa el *ErrorDocument 401* (la petició requereix d'autenticació), cal fer referència a una *URL* local, ja que si es redirigeix a un altre lloc web, al tenir un error d'autenticació no proporcionarà el contingut web.
Exemples:
`ErrorDocument 500 http://www.gencat.net/err_intern.html`
`ErrorDocument 403 "Accés no permès"`
Per veure els diferents codis d'error es pot consultar:
	C I D

http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html	

C28. La directiva *ServerTokens* permet la configuració de les capçaleres de resposta *HTTP*. Cal configurar-ho a *Prod* per evitar que s'informi de la versió completa de servidor *Apache* que s'està utilitzant:
`ServerTokens Prod`
Si no es configura la directiva, per defecte s'informa de la configuració completa del servidor web com mostra el següent exemple:
`Server: Apache/2.0.41 (Unix) PHP/4.2.2 MyMod/1.2`
	C I D

C29. No es podran activar els tipus de dades *MIME* que permetin la descompressió de fitxers "al vol" pels problemes de seguretat que presenta, ja que implica que en el servidor web es desempaquetin automàticament fitxers comprimits.
`x-gzip .gz`
`x-compress .Z`
	I D

C30. Configurar el mòdul *SSL mod_ssl* per a poder utilitzar *HTTPS* per accedir al servidor web si és necessari. Utilitzar protocols robustos SSL v3 i TLS v1 i claus de com a mínim 128 bits:
`SSLProtocol -all +TLSv1 +SSLv3`
`SSLCipherSuite HIGH:MEDIUM:!aNULL:+SHA1:+MD5:+HIGH:+MEDIUM`
	C I

C31. 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 D

Recomanacions

R2. Configurar les directives que limiten els recursos que consumeix *Apache* i així evitar que el servidor es quedi sense memòria o CPU. En principi els valors per defecte són suficients, però pot haver-hi entorns on calgui modificar algun dels paràmetres. Les directives són:

```
LimitRequestBody bytes
LimitXMLRequestBody bytes
LimitRequestFields number
LimitRequestFieldSize bytes
LimitRequestLine bytes

RLimitCPU seconds|max
RLimitMEM bytes|max
RLimitNPROC number|Max
```

També existeixen directives per a controlar els recursos destinats a atendre peticions web al servidor:

```
MaxKeepAliveRequests
MinSpareThreads
MaxSpareThreads
ThreadLimit
ServerLimit
MaxClients
LimitInternalRecursion
```

R3. Instal·lar el mòdul *modsecurity*. És un mòdul de codi lliure que proporciona seguretat a nivell d'aplicació web. Detecta i preveu atacs analitzant les peticions abans que arribin a l'aplicació.

4.3. MN - Monitoratge

OBJECTIUS	
Registrar totes les peticions de contingut web que es realitzin en el servidor. A part de detectar anomalies o possibles atacs, també serviran per a obtenir estadístiques d'ús dels llocs web.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C32. Caldrà donar compliment als requeriments de la *Norma de gestió de traces* per a	C I

garantir la traçabilitat i custòdia dels esdeveniments dels sistemes.	
C33. 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
C34. Qualsevol possible incident de seguretat haurà de ser comunicat en la major brevetat possible mitjançant el *Procediment de notificació d'incidents de seguretat*.	C I
C35. Protegir el directori *logs* perquè només hi tingui privilegis d'escriptura l'usuari *root*.	I

Recomanacions

R1. Es recomana, revisar periòdicament les traces per a detectar activitats anòmales que puguin comprometre la seguretat del sistema.

R2. Per les traces d'error es recomana establir el nivell als avisos de perill (*warning*):

```
LogLevel warn
```

Informació generació traces Apache

Per les traces d'accés utilitzar el format *common* que garanteix que es guarda la informació mínima necessària. És la configuració per defecte:

```
LogFormat "%h %l %u %t \"%r\" %>s %b" common
```

Adequar els paràmetres en funció dels requeriments de la *Norma de gestió de traces.*

4.4. CA - Control d'accés i privilegis.

OBJECTIUS	
Especificar els mecanismes de què disposa *Apache* per a realitzar l'identificació, autenticació i control d'accés als continguts web que serveix el servidor web. L'autenticació fa referència a la pròpia que proporciona el servidor *Apache*, no a la que pugui estar implantada per les aplicacions, que d'altra banda, és l'opció recomanable.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C36. Utilitzar les directives *Allow* i *Deny* per a habilitar o inhabilitar l'accés des de certs hosts o adreces IP.	C
C37. En les aplicacions, evitar utilitzar l'autenticació pròpia d'Apache i implementar-la a través de l'aplicació web.	C I
C38. En cas d'utilitzar l'autenticació pròpia, *Apache* proporciona una utilitat per a la gestió d'usuaris i contrasenyes. Per defecte la informació es guarda en un fitxer. Per grans volums d'usuaris és aconsellable utilitzar un gestor de base de dades per a emmagatzemar els usuaris i contrasenyes. Utilitzar la següent directiva per especificar l'accés a una base de dades per a l'obtenció dels usuaris i contrasenyes: `AuthBasicProvider dbm` De totes maneres, si són pocs els usuaris a donar d'alta pel control d'accés, es podrà utilitzar el fitxer de contrasenyes. Generar-lo amb l'utilitat *htpasswd* i es recomana ubicar-lo on resideixi la instal·lació del servidor. Mai estarà en un directori accessible a través del servidor web.	C I
C39. En cas d'utilitzar l'autenticació pròpia, mitjançant la directiva *AuthType*, s'especifica com es realitzarà l'autenticació de l'usuari per accedir a un contingut web. Existeixen dos mètodes: • *Basic (mod_auth_basic)*: No està permès usar-lo perquè fa la transferència de les dades d'identificació en clar, a no ser que la comunicació es faci sobre *HTTPS*. • *Digest (mod_auth_digest)*: Utilitza l'algorisme *MD5* per a obtenir el *hash* i realitzar l'enviament d'aquest enlloc d'enviar les dades en clar.	C I

Degut als problemes de compatibilitat amb els navegadors de Digest, utilitzar el mètode “Basic” implementant la fase d’autenticació via *HTTPS*.	
C40. En cas d’utilitzar l’autenticació pròpia, configurar la directiva *AuthName* amb un nom identificatiu de l’àrea (*realm*) en la que s’està demanant accés. Aquesta informació es la que apareixerà en el navegador del client quan se li sol·liciti l’usuari i contrasenya.	C I

4.5. 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**
C41. Caldrà facilitar les tasques d’auditoria per part de l’Oficina de Seguretat davant a la revisió del compliment dels requeriments de seguretat marcats pel CTTI.	C I D

4.6. 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 serveis basats en servidor web Apache	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C42. Es recollirà contractualment el compliment de les normes i guies que el CTTI tingui per l’entorn *Apache* així com qualsevol altra norma de gestió o administració que sigui d’aplicació.	C I D
C43. Es garantirà el compliment de la *Norma de contractació de tercers*.	C I D
C44. 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 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 cada 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

CGI: *Common Gateway Interface*. Connector que passa la informació capturada en una pàgina web cap a una aplicació per al seu processament i rebre dades de l'aplicació per passar-les al client web.

HTML: *Hypertext Markup Language*. Llenguatge que permet mostrar la informació a través d'un navegador web.

HTTPS: *HTTP* sobre *SSL*. Protocol de transmissió segura de contingut web.

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).

Script: conjunt d'instruccions tècniques a executar en un sistema de manera automàtica.

SSI: *Server Side Includes*. Directives incloses en pàgines *HTML*, i avaluades en el servidor quan es serveixen les pàgines. Permeten afegir parts de contingut generat dinàmicament en una pàgina estàtica en HTML, sense necessitat de servir la pàgina sencera mitjançant un *CGI* o un altre sistema de generació dinàmica de pàgines web.

SSL: *Secure Socket Layer*. Protocol per a aportar seguretat en la transmissió de missatges per Internet.

10 DOCUMENTACIÓ REFERENCIADA

- GE-GUI07 Guia protecció entorns Linux
- GE-GUI08 Guia protecció entorns Solaris
- GE-GUI27 Guia de protecció entorns HP-UX
- GE-GUI32 Guia protecció entorns AIX
- GE-GUI10 Guia protecció entorns Windows 2003
- GE-GUI40 Guia de còpies de seguretat
- GE-PRO01 Procediment de notificació d'incidents de seguretat
- GE-GUI19 Guia de contrasenyes
- GE-GUI20 Guia de gestió de comptes d'administrador de sistemes
- CT-NOR03 Norma de contractació de tercers
- Pla d'auditories de seguretat
- Pàgina web del servidor Apache: http://httpd.apache.org
- Mòdul modsecurity: http://www.modsecurity.org/

11 PARAULES CLAU

Apache, servidor web, SSI, CGI, HTTPS, SSL, 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.