ÍNDEX

RESUM 2
1 OBJECTIU 3
2 ÀMBIT I VIGÈNCIA 3
3 COMPLIMENT AMB ELS REQUISITS LEGALS I ESTÀNDARDS DE SEGURETAT 4
4 DESCRIPCIÓ DELS CONTROLS 4
4.1. IN – Instal·lació i manteniment 4
4.2. CN - Configuració 5
4.3. MN - Monitoratge 7
4.4. CA - Control d'accés i privilegis 8
4.5. AU - Auditoria 8
4.6. OU - Outsourcing o subcontractació del servei 8
5 CONTROL 9
6 PENALITZACIONS 9
7 DIVULGACIÓ 9
8 REVISIÓ 9
9 GLOSSARI DE TERMES 9
10 DOCUMENTACIÓ REFERENCIADA 10
11 PARAULES CLAU 10
12 HISTÒRIC DEL DOCUMENT 10
13 ANNEX A – Components del servidor IIS 11
14 ANNEX B – Configuració traces del servidor IIS 13
15 ANNEX C – Configuració segura de WebDAV 15

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	5/10/10/2009	6/10/2009

Estàndard signat digitalment pel:
Generalitat de Catalunya
Centre de Telecomunicacions i Tecnologies de la Informacio
Estàndard aprovat
Barcelona
2009.10.06 12:17:41 +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 IIS amb l'objectiu de garantir la confidencialitat, integritat i disponibilitat de la informació i serveis suportats per aquesta plataforma.

ÀMBIT

Servidors web IIS de la Generalitat de Catalunya.

DESCRIPCIÓ

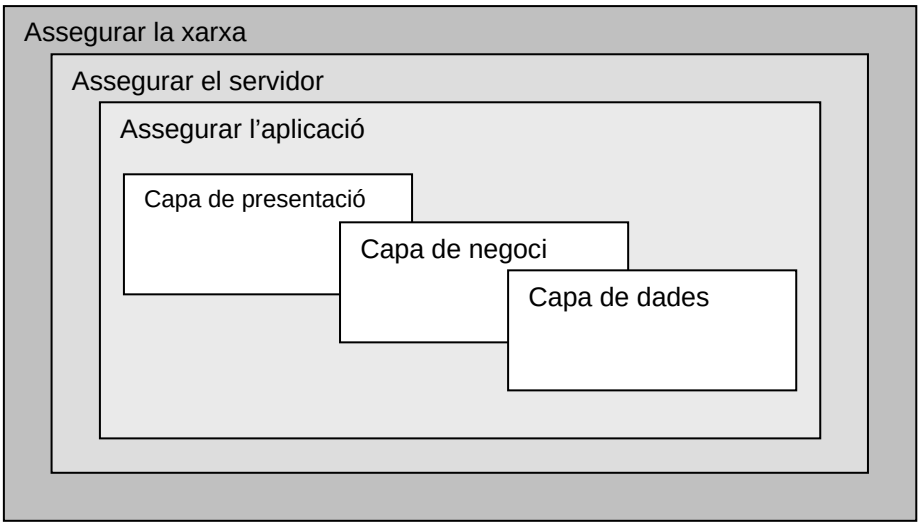
Es recullen els controls de seguretat orientats a garantir la confidencialitat, privacitat, integritat i disponibilitat de la informació de sistemes basat en Servidors web IIS.

1 OBJECTIU

Definir els controls per administrar i gestionar la seguretat en els equips que tenen instal·lat l'IIS.

IIS engloba una sèrie d'eines administratives que permeten controlar llocs Web, FTP, SMTP i serveis de notícies. També dona el suport necessari per a la creació de pàgines dinàmiques (ASP).

Per tal de tenir aplicacions segures, s'han assegurar cada una de les seves parts:



No es l'objectiu d'aquesta guia explicar com es protegeixen cada una de les parts, però sí que es vol recalcar la importància de fer-ho a tots els nivells, per tal de tenir un entorn completament segur.

La forma de protegir IIS depèn de la versió de Windows que s'estigui executant. Microsoft ha desenvolupat algunes eines per ajudar en la tasca de protecció: *IIS Lockdown Wizard* és una eina disponible per a Windows 2000; Windows NT; Windows XP; que desactiva tots els serveis innecessaris de l'ISS 4.0, 5.0, 5.1 respectivament per tal d'incrementar la seva seguretat. Es pot descarregar del centre de descarregues de Microsoft:

(http://www.microsoft.com/downloads/details.aspx?FamilyID=dde9efc0-bb30-47eb-9a61-fd755d23cdec&DisplayLang=en).

IIS Lockdown Wizard no està disponible per a Windows Server 2003 però es pot executar *URLScan* per a protegir IIS en Windows Server 2003. *URLScan* es una altre eina que restringeix els tipus de sol·licituds HTTP que l'IIS processarà. Al bloquejar determinades sol·licituds HTTP, *URLScan* ajuda a evitar que arribin al servidor sol·licituds que puguin resultar perilloses. A més permet el canvi de directori dels arxius de log i el logging de URLs llargs (Logging log URLs)

En aquesta guia no es contemplen versions inferiors a IIS 4.0. Es recomana que, en cas de tenir aplicacions instal·lades en versions inferiors, aquestes siguin actualitzades.

IIS 6.0 no està instal·lat per defecte en els sistemes operatius de la família *Microsoft Windows Server 2003*. A diferència de les versions anteriors, s'instal·la amb el mínim de components necessaris (servir contingut estàtic).

Tots els canvis proposats en aquesta guia han de ser primer instal·lats en un entorn de desenvolupament i s'ha fer un test exhaustiu de les aplicacions per tal d'assegurar que tot continua funcionant normalment.

2 ÀMBIT I VIGÈNCIA

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

La versió actual entrarà en vigor el dia 6 d'octubre 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
- 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
- 11.5.3 Sistema de gestió de les contrasenyes
- 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 possibles controls de seguretat orientats a garantir la confidencialitat, privacitat, integritat i disponibilitat de la informació. Aquests s'agrupen per grups d'accions o procediments operatius orientats a combatre les amenaces a les quals un equip amb *IIS* està exposat. L'aplicació d'un conjunt ampli dels controls d'una manera lògica, ordenada i planificada reduirà progressivament les vulnerabilitats del sistema i, per tant, l'exposició als riscos. 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	
Requisits en la instal·lació, actualització i manteniment del servidor *IIS*. S'han de mantenir actualitzats tots els components del sistema (Windows, en la versió que sigui, IIS, .NET Framework i MDAC (Microsoft Data Access Components)).	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C1. Quan calgui instal·lar un nou servidor IIS, s'ha d'optar per una versió que tingui suport per part del fabricant i actualitzada amb els corresponents pegats de seguretat.	I D
C2. Activar només les extensions necessàries (per a generar contingut dinàmic) del servidor per al funcionament dels aplicatius.	C I D
C3. Instal·lar els mínims components del servidor IIS necessaris. En l'annex A es detallen els components, la seva finalitat així com l'estat recomanat per defecte de cada mòdul.	C I D
C4. Instal·lar els servidors en màquines dedicades.	I D
C5. No fer instal·lacions en controladors de domini.	I D
C6. No donar accés públic al servidor fins que es trobi convenientment protegit.	C I D
C7. És important mantenir actualitzat el sistema operatiu segons la *Guia protecció entorns Windows 2003*.	C I D
C8. 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
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. Per versions de IIS 5.0 o menors es recomana instal·lar l'utilitat IIS LockDown. Es pot aconseguir a: http://download.microsoft.com/download/iis50/Utility/2.1/NT45XP/EN-US/iislockd.exe

IIS LockDown ajuda a reduir les vulnerabilitats de les instal·lacions Windows 2000 Server. A més instal·la una eina anomenada URLScan que ajuda als administradors a restringir el tipus de peticions http que el servidor pot processar, basant-se en una sèrie de regles que l'administrador controla.

IIS LockDown crea un log amb totes les modificacions que fa. Tots els canvis que faci IIS LockDown són reversibles.

L'última versió (2.1) de IIS Lockdown Wizard treballa amb Windows 2000, Windows NT, Windows XP, Windows NT 4.0 executant IIS 4.0, Windows 2000 executant IIS 5.0 o Windows XP executant IIS 5.1

R2. Per versions de IIS 5.0 o menors es recomana la instal·lació de URLScan. Una vegada baixat el IIS LockDown, executar: *iislockd.exe /q /c* per extreure URLScan.

URLScan funciona amb plantilles configurables que permeten definir quines sol·licituds HTTP no es processaran. Per exemple, bloqueja totes les peticions que contenen caràcters que l'administrador consideri perillosos, com ".." i escriu totes aquestes peticions en un fitxer de log.

R3. Si existeixen servidors amb versions anteriors a la 6.0 en màquines d'explotació és molt recomanable planificar una migració a versions més actuals.

4.2. CN - Configuració

OBJECTIUS	
Deshabilitar tots els serveis Windows no utilitzats, protocols poc segurs, protegir tots els fitxers i directoris que continguin informació sensible ...	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C10. Per a la transmissió de fitxers, no es pot utilitzar FTP. S'han d'utilitzar alternatives com la instal·lació d'un servidor de SFTP o bé WebDAV degudament configurat.	C I D
C11. IIS suporta WebDAV (estàndard que descriu com copiar, moure, modificar les seves propietats... fitxers a través del protocol HTTP). Deshabilitar aquesta opció als servidors de producció en cas de no ser necessària. Això es pot fer a través del IIS LockDown. A la versió 6.0 del IIS ja ve deshabilitada per defecte. En l'annex C de la guia es recullen els requeriments de securització per WebDAV en cas de ser necessari utilitzar-lo.	C I D
C12. Configurar el servidor per a poder utilitzar *HTTPS* per accedir al servidor web. Utilitzar protocols robustos SSL v3 i TLS v1 i claus de com a mínim 128 bits.	C I D
C13. Les utilitats SDK no han d'estar instal·lades en els entorns de producció.	C I D
C14. Treure les comparticions de carpetes no necessàries, utilitzant l'opció *Carpetes Compartides* de l'eina *Administració d'Equips* (MMC) que es troba entre les E*ines Administratives* del P*anell de Control*.	C I D
C15. Moure el lloc Web a una unitat que no sigui del sistema. No utilitzar el directori per defecte *\inetpub\Wwwroot* com a ubicació del contingut del lloc Web. Per exemple, si el sistema s'instal·la a l'unitat C:, pot moure el directori del contingut a la unitat D:	C I D
C16. Deshabilitar l'ús de ".." per a prevenir atacs transversals: - Arrencar l'IIS - Prémer el botó dret a l'arrel del lloc Web i seleccionar *Propietats* - Seleccionar la pestanya *Directori Principal* i prémer sobre *Configuració* - Seleccionar la pestanya *Opcions d'aplicació* - Seleccionar *Habilitar rutes d'accés primàries*	C I D
C17. Esborrar tots els directoris virtuals potencialment perillosos: les aplicacions d'exemple no haurien d'instal·lar-se als servidors de producció. Esborrar totes les aplicacions d'exemple, incloent les que només poden ser accedides des de la màquina local amb http://localhost, or http://127.0.0.1. Esborrar també els següents directoris virtuals dels servidors de producció: IISSamples, IISAdmin, IISHelp i *Scripts*.	C I D
C18. Esborrar o assegurar (en cas de que no es pugui esborrar) el Remote Data Services (RDS), component que permet l'accés remot i podria permetre a un intrús executar codi al servidor.	C I D

- Esborrar RDS: és el millor en cas que les aplicacions instal·lades al servidor no l'utilitzin. Per a fer-ho: - Esborrar el directori virtual /MSADC - Esborrar els fitxers i subdirectoris RDS de \Program Files\Common Files\System\Msadc - Esborrar la següent clau del registre: HKLM\System\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch - Nota: Encara que l'IISLockDown te una opció per a esborrar el directory virtual MSADC, no esborra la clau del registre - Assegurar RDS: en cas que les aplicacions sí que utilitzin RDS, es poden fer algunes coses per a fer-ho més segur: - Esborrar tots els exemples de Progam Files\Common Files\System\Msadc\Samples - Esborrar la següent clau del registre: HKLM\System\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch \VbBusObj.VbBusObjCls - Deshabilitar l'accés anònim al directori virtual del MSADC a l'ISS - Crear a HKLM\Software\Microsoft\DataFactory\HandlerInfo\ una nova clau de registre HandlerRequired, de tipus DWord i valor 1	
C19. No es permet l'ús de les FPSE (FrontPage Server Extensions) per a la publicació de contingut.	C I D
C20. Mapejar les extensions de fitxer de l'IIS: algunes de les extensions de fitxer incloses a l'IIS són: .asp, asa, .cer, .cdx, .htr, .idc, .shtm, .shtml... Per a versions inferior a la 6.0, és recomanable assignar una ruta d'accés executable per defecte 404.dll (proporcionada per l'IIS LockDown) a les que no s'utilitzin.	C I D
C21. Mapejar les extensions dels fitxers de *.NET Framework* que no es vulgui que els usuaris puguin cridar associant-los al System.Web.HttpForbiddenHandler del machine.config. Per a versió 2.0 de *.NET* o superiors l'arxiu de configuració és web.config.	C I D
C22. Esborrar tots els filtres ISAPI que no utilitzi l'aplicació.	C I D
C23. Restringir l'accés a la metabase d'IIS, utilitzant permisos *NTFS*: al directori *\WINNT\system32\inetsrv* seleccionar l'arxiu *Metabase.bin* (Metabase.xml per a la versió 6.0) i des de la pestanya de seguretat treure tots els permisos de l'arxiu i concedir "*control total*" només als usuaris LocalSystem i Administradors.	C I D
C24. Restringir l'accés al fitxer *machine.config* (*.NET* 1.0) i web.config (*.NET* 2.0 o superiors) només als usuaris LocalSystem i Administradors.	C I D
C25. Utilitzar la classe *HttpForbiddenHandler* per a evitar la descàrrega de determinats tipus d'arxius a través de la web, com ara arxius de configuració. Es troba a la secció *<httpHandlers>* de l'arxiu *machine.config*. Per a versió 2.0 de *.NET* o superiors l'arxiu de configuració és web.config.	C I D
C26. Verificar que les traces de depuració de programa (*debug*) estan deshabilitades en els entorns de producció. Per a fer-ho, obrir l'arxiu *machine.config* i posar a l'etiqueta *trace*: *<trace enabled="false" ....>*. Per a versió 2.0 de *.NET* o superiors l'arxiu de configuració és web.config.	C I D
C27. Verificar que l'atribut *debug* de l'etiqueta de compilació està a deshabilitat. Per a fer-ho, obrir l'arxiu *machine.config* i posar a l'etiqueta *<compilation debug="false"...>*. Per a versió 2.0 de *.NET* o superiors l'arxiu de configuració és web.config.	C I D
C28. Per a què els errors no es mostrin als usuaris, si no que els aparegui una pàgina d'error genèrica, modificar l'etiqueta customErrors de l'arxiu *machine.config* indicant quina és la pàgina d'error a mostrar *<customErrors mode="On" defaultRedirect="Pàgina_Error_Genèrica.htm" />*. Per a versió 2.0 de *.NET* o superiors l'arxiu de configuració és web.config.	C I D
C29. Modificar les pàgines d'error perquè no s'informi de la versió del servidor. Al seu lloc, s'haurà de mostrar una pàgina d'error prèviament definida.	C I D
C30. Treure tots els permisos de la zona Intranet Local seguint els següents passos: • Inicialitzar l'eina de configuració de Microsoft *.NET* Framework des de les eines	C I D

administratives. • Expandir Runtime Security Policy, expandir Machine, expandir *Code Groups*, expandir *All_Code* i seleccionar *LocalIntranet_Zone*. • Prémer *Edit Code Group Properties*. • Prémer la pestanya *Permission Set*. • Seleccionar *Nothing* de la llista de permisos. • Prémer Acceptar.	
C31. Treure tots els permisos de la zona Internet: la zona Internet aplica permisos d'accés al codi baixat d'Internet. • Inicialitzar l'eina de configuració de Microsoft *.NET* Framework des de les eines administratives. • Expandir Runtime Security Policy, expandir Machine, expandir *Code Groups*, expandir *All_Code* i seleccionar *Internet_Zone*. • Prémer *Edit Code Group Properties*. • Prémer la pestanya *Permission Set*. • Seleccionar *Nothing* de la llista de permisos. • Prémer acceptar	C I D
C32. 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

R4. Executar el comandament "*caspol –s On*" per a activar la seguretat d'accés a codi. Caspol (Code Access Security Policy Tool) és una eina per entorns *.NET* que permet aplicar polítiques de seguretat.

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**
C33. 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
C34. 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
C35. 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
C36. Els fitxers de traces que es creïn com a resultat de l'auditoria, s'han de protegir amb permisos *NTFS* de forma que no puguin ser modificats o esborrats en cas d'atac. Afegir els següents permisos a cada una de les carpetes i subcarpetes: - Administradors: Full Control - System: Full Control - Backup Operators: Read	I
C37. Es generaran els fitxers de traces per cada un dels servidors virtuals en funcionament.	I

Recomanacions

R5. Es recomana revisar periòdicament les traces per a detectar activitats anòmales que puguin comprometre la seguretat del sistema.

R6. Moure i reanomenar tots els fitxers de traces de l'IIS per a dificultar que els intrusos puguin amagar/modificar proves.

4.4. CA - Control d'accés i privilegis

OBJECTIUS	
Deshabitar tots els comptes que no siguin necessaris, reforçar la política de contrasenyes i aplicar el principi de mínim privilegi als comptes d'usuaris.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C38. Deshabilitar tots els comptes d'usuari que no s'utilitzin. Si passat un temps prudencial des de la deshabilitació del compte no apareix cap problema que faci pensar que era utilitzat, esborrar-lo (els comptes esborrats no són recuperables).	C I
C39. Deshabilitar el compte de convidat (*Guest*). En algunes versions d' IIS es deshabilita per defecte. Per a comprovar el seu estat, utilitzar l'eina *Administració d'Equips* (Microsoft Management Console - MMC) que es troba entre les *Eines Administratives* del *Panell de Control*. Si a l'opció *Usuaris* el compte *Invitat* té una creu vermella a sobre, és que està deshabilitat.	C I
C40. Treure permisos d'accés als usuaris *Everyone* als següents directoris: - Arrel (\) - Directoris de sistema (\WINNT\system32) - Directoris d'eines del *.NET* Framework *(\WINNT\Microsoft.NET\Framework\{version})* - Directori arrel i directoris de contingut de l'aplicació (per defecte és \inetpub*)	C I D
C41. Restringir l'accés de l'usuari *Anònim*: - Denegar l'accés d'escriptura als directoris amb contingut de l'aplicació. - Restringir l'accés a les eines de sistema que s'executen des de línia de comandes (\WINNT\system32).	C I D
C42. Utilitzar diferents comptes d'usuari per a les diferents aplicacions instal·lades.	C I D
C43. En les aplicacions, evitar utilitzar l'autenticació pròpia de l'IIS i implementar-la a través de l'aplicació web.	C I
C44. En cas d'utilitzar l'autenticació pròpia, utilitzar l'autenticació integrada amb el sistema operatiu Windows o l'autenticació bàsica xifrant la comunicació via *HTTPS*.	C I
C45. Donar compliment a la política de contrasenyes segons la *Norma contrasenyes* disponible.	C I
C46. Restringir les connexions remotes a només els usuaris que realment necessitin fer-ho.	C I

4.5. AU - Auditoria

OBJECTIUS	
Tenir activats els mecanismes d'auditoria pot ajudar a fer el seguiment d'atacs. A continuació, la llista d'esdeveniments que s'haurien d'auditar:	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C47. 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 IIS.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C48. Es recollirà contractualment el compliment de les normes i guies que el CTTI tingui per l'entorn *IIS* així com qualsevol altra norma de gestió o administració que sigui d'aplicació.	C I D
C49. Es garantirà el compliment de la *Norma de contractació de tercers*.	C I D
C50. 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 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

NTFS: Acrònim de NT File System. És un sistema d'arxius dissenyat específicament per a Windows NT, que millora la funcionalitat dels sistemes anteriors.

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

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).

SP: Acrònim de *Service Pack*. Actualitzacions de programari que distribueix Microsoft per a solucionar vulnerabilitats detectades en el programari del sistema operatiu.

.NET: Entorn que permet dotar de funcionalitat de servidor d'aplicacions per a entorns web sobre arquitectures Windows (homòleg a l'estàndard J2EE de Sun per entorns Unix).

10 DOCUMENTACIÓ REFERENCIADA

- GE-GUI10 Guia protecció entorns Windows 2003
- GE-GUI40 Guia de còpies de seguretat
- GE-PRO01 Procediment de notificació d'incidents de seguretat
- GE-GUI19-02 Guia de contrasenyes
- GE-GUI20 Guia de gestió de comptes d'administrador de sistemes
- CT-NOR03 Norma de contractació de tercers
- GE-PRO01 Procediment de notificació d'incidents de seguretat
- Pla d'auditories de seguretat

Recursos Microsoft:

- http://www.microsoft.com
  - MBSA http://www.microsoft.com/technet/security/tools/mbsahome.mspx
  - IIS Lockdown http://download.microsoft.com/download/iis50/Utility/2.1/NT45XP/EN-US/iislockd.exe
  - IIS 6.0 Resource Kit Tools: http://www.microsoft.com/downloads/details.aspx?FamilyID=56fc92ee-a71a-4c73-b628-ade629c89499&displaylang=en
- http://technet.microsoft.com/es-es/library/cc782762.aspx
- http://technet.microsoft.com/es-es/library/cc753198.aspx

11 PARAULES CLAU

Windows, administració, usuaris, grups, permisos, pegat de seguretat, IIS, 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.

13 ANNEX A – Components del servidor IIS

A continuació s'indiquen els diferents mòduls amb l'estat recomanat per defecte.

Components del servidor d'aplicacions:

Component	Descripció	Estat recomanat per defecte
Application Server Console	Proporciona un punt central des del que administrar les aplicacions. En lloc de l'*Application Server Console*, utilitzar *IIS Server Manager.*	Deshabilitat
ASP.NET	Proporciona suport a aplicacions ASP.NET. Habilitar només quan a l'IIS corrin aplicacions ASP. NET.	Deshabilitat
Enable Network COM+ Access	Permet al servidor IIS executar aplicacions que utilitzen components COM+ per aplicacions distribuïdes. Es necessari, entre altres per *FTP*, *BITS Server extension*, *WWW* i *IIS Manager*.	Habilitat
Enable Network DTC Access	El coordinador de transaccions distribuïdes (DTC) permet coordinar les transaccions que utilitzen dos o més recursos protegits contra transaccions com bases de dades, cues, arxius de sistema, etc. Habilitar només quan les aplicacions ho requereixin.	Deshabilitat
Internet Information Service (IIS)	Oferix serveis web i FTP bàsics. Aquest component és necessari per als servidors IIS dedicats. Si no està habilitat aquest component, es deshabiliten tots els subcomponentes.	Habilitat
Message Queing	Quan està deshabilitat, també ho estan tots els seus components.	Deshabilitat

Components de l'IIS:

Component	Descripció	Estat recomanat per defecte
Background Intelligent Transfer Service (BITS)	Servei de transferència intel·ligent en segon pla. Es un mecanisme de transferència d'arxius en segon pla, així com un administrador de cues.	Deshabilitat
Arxius Comuns (*Common Files*)	IIS necessita aquest fitxers i per això han d'estar sempre habilitats.	Habilitat
Servei FTP	Permet al servidor IIS proveir serveis FTP. Aquest servei no és necessari per als servidors IIS dedicats.	Deshabilitat
Extensions de servidor Front Page 2002	Proporciona compatibilitat amb FrontPage per administrar i publicar llocs. Habilitar només quan les aplicacions ho requereixin.	Deshabilitat
Internet Information Services Manager	Permet l'administració de l'IIS	Habilitat
Internet Printing	Serveis d'impressió i compartició d'impressores. Normalment no serà necessari. Aquest component no és necessari en els servidors IIS dedicats.	Deshabilitat
NNTP Service	Proporciona servei de grups de noticies Usenet en Internet. Aquest component no és necessari en els servidors IIS dedicats.	Deshabilitat
SMTP Service	Mòdul per a la creació d'un servei de transferència de missatges o SMTP. Habilitar només quan les aplicacions ho requereixin.	Deshabilitat

	Aquest component no és necessari en els servidors IIS dedicats.	
World Wide Web Service	Servei de publicació de pàgines web. Aquest component és necessari en els servidors IIS dedicats.	Habilitat
Conector de dades d'Internet	Proporciona compatibilitat per al contingut dinàmic que es proporciona a través dels arxius amb extensions .idc. També es pot des habilitar mitjançant les extensions del servei web	Deshabilitat
Administració remota (HTML)	Proporciona una interface HTML per a administrar IIS. Utilitzar l'Administrador d'IIS per a facilitar l'administració i reduir la superfície d'atac d'un servidor IIS. Aquesta funció no és necessària en els servidors IIS dedicats.	Deshabilitat
Connexió web a escriptori remot	Inclou el control ActiveX® de Microsoft i pàgines de mostra per a allotjar connexions de client de Serveis de Terminal Server. Utilitzi l'Administrador d'IIS per a facilitar l'administració i reduir la superfície d'atac d'un servidor IIS. No és necessari en un servidor IIS dedicat.	Deshabilitat
Inclusió del servidor	Oferix compatibilitat per als arxius .shtm, .shtml i .stm. Deshabilitar aquest component si cap dels llocs ni aplicacions web que s'executen en un servidor IIS inclou arxius amb aquestes extensions.	Deshabilitat
WebDAV	WebDAV amplia el protocol HTTP/1.1 per a permetre als clients publicar, bloquejar i administrar recursos en la Web. Deshabilitar aquest component en els servidors IIS dedicats. També pot ser deshabilitat mitjançant les extensions del servei web	Deshabilitat

14 ANNEX B – Configuració traces del servidor IIS

Auditar tots els intents de connexió erronis.

- Obrir la *Directiva de Seguretat Local* que es troba entre les *Eines Administratives* del *Panell de Control*
- A *Directives Locals*, seleccionar *Directives d'auditoria*
- Prémer a *Auditar esdeveniments d'inici de sessió de compte*
- Prémer a *Fallida* i després a *Acceptar*

Els errors de connexió s'emmagatzemen al "*Visor de sucesos*", pestanya de Seguretat. Aquestes són les respostes sospitoses que podem trobar :

529	Intent d'inici de sessió amb un nom d'usuari desconegut o amb un nom d'usuari conegut i una contrasenya incorrecta.
531	Intent d'inici de sessió amb un compte desactivat.
532	Intent d'inici de sessió amb un compte caducat.
533	L'usuari no te permís per a iniciar la sessió en aquest equip.
534	L'usuari ha intentat iniciar la sessió amb un tipus d'inici de sessió no permès (de xarxa, interactiu, per lots, de serveis o interactiu remot).
537	Error d'intent d'inici de sessió per altres raons.
539	El compte s'ha bloquejat quan s'ha intentat iniciar la sessió. Aquest succés pot indicar un atac de contrasenyes que fa que el compte es bloquegi.

Registrar les accions fallides sobre el sistema de fitxers

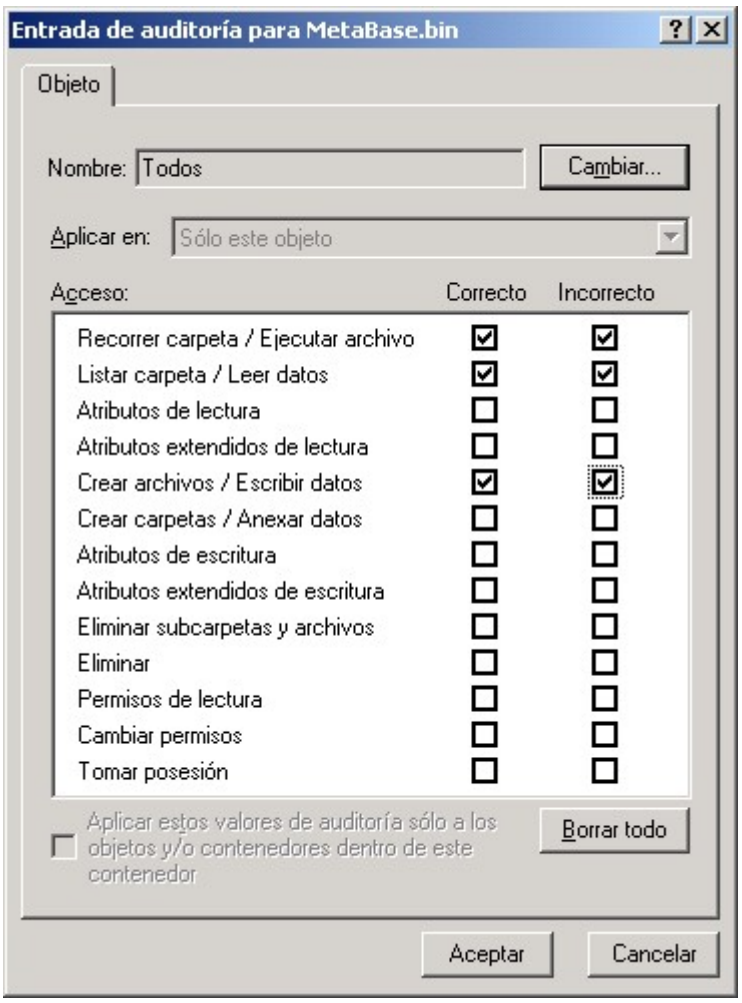
- Obrir la *Directiva de Seguretat Local* que es troba entre les *Eines Administratives* del *Panell de Control*
- A *Directives Locals*, seleccionar *Directives d'auditoria*
- Prémer a *Directives d'accés a objectes*
- Prémer a *Fallida* i després a *Acceptar*

Per a auditar el sistema de fitxers:

- Des de l'explorador de Windows, situar-se a l'arrel del sistema de fitxers
- Prémer al botó dret del ratolí i seleccionar *Propietats*
- Anar a la pestanya de *Seguretat*
- Prémer sobre *Opcions Avançades* i obrir la pestanya *Auditar*
- Prémer a *Afegir* i escriure *Everyone* en el camp nom. Prémer Acceptar
- Seleccionar totes les opcions per a auditar tots els esdeveniments. Per defecte, afecta a totes les carpetes, subcarpetes i fitxers.
- Seleccionar *Acceptar* fins a tancar totes les finestres obertes.

Auditar els accessos al fitxer Metabase.bin (Metabase.xml per a versions IIS 6.0), que conté informació de la configuració de l'IIS

- Buscar l'arxiu *C:\WINNT\system32\inetsrv\MetaBase.bin*, prémer al botó dret del ratolí i seleccionar *Propietats*
- Seleccionar la pestanya *Seguretat*, prémer a *Avançades*, *Auditoria* i a *Afegir*
- Seleccionar *Everyone*, prémer a *Afegir* i després *Acceptar*.
- Seleccionar, per a tots els tipus d'accés, *Erroni* i després premi *Acceptar*:



Fer la mateixa operació a la carpeta a on es guarden les còpies de seguretat del fitxer Metabase.bin

15 ANNEX C – Configuració segura de WebDAV

WebDAV és un component del IIS que permet la publicació remota de contingut web. En cas d'utilitzar-se, cal tenir en compte els següents requeriments:

- No habilitar l'accés anònim al directori de publicació de continguts.
- Configurar els permisos sobre els fitxers de la carpeta de publicació de forma adequada, garantint sempre el principi de mínims privilegis.
- Inhabilitar l'execució d'scripts en la carpeta si no és necessari.