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	QSRaP	27/07/2009	31/07/2009

Estàndard signat digitalment pel:
Generalitat de Catalunya
Centre de Telecomunicacions i Tecnologies de la Informacio
Estàndard aprovat
Barcelona
2009.07.27
10:53:33 +02'00'

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

RESUM

OBJECTIU

Definir els controls a aplicar per a la protecció d'entorns *SQL Server*, amb l'objectiu de garantir la confidencialitat, integritat i disponibilitat de la informació i serveis suportats per aquesta plataforma.

ÀMBIT

Bases de dades *SQL Server* 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 SQL Server.

1 OBJECTIU

Definir els controls per instal·lar, administrar i gestionar la seguretat dels equips que tenen instal·lat SQL Server en producció d'una manera segura, que garanteixi la confidencialitat, integritat i disponibilitat dels serveis implantats amb aquesta plataforma als Serveis Centrals de la Generalitat de Catalunya. No és l'objectiu d'aquesta guia indicar com administrar i gestionar SQL Server.

Aquesta guia està centrada en SQL Server 2000 i 2005. Per versions anteriors, molts d'aquests controls també serveixen, però pot variar la forma d'implementar-los.

Tots els controls 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 d'instal·lació, explotació i manteniment de les bases de dades SQL Server 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.

L'àmbit d'aquesta guia se cenyeix als entorns d'explotació de bases de dades SQL Server. No afecta a entorns de proves o integració, ja que moltes de les configuracions poden estar habilitades per qüestions de proves o desenvolupament.

La guia ha estat redactada tenint en compte les recomanacions de seguretat per a les versions SQL Server 2000 i 2005. Si algun control només aplica a una de les versions, s'indica en el propi control.

A més d'aquesta guia, s'hauria de complir allò que estigui establert a qualsevol altra guia d'administració de sistemes en general, ja que en aquesta guia s'identifiquen els controls específics per garantir un mínim de seguretat en els equips amb SQL Server, però no per administrar el sistema en sí.

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

La guia és d'obligat compliment en l'àmbit dels *Serveis TIC Centrals*.

Entrarà en vigor el dia 1 d'agost 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 17799:2005:

- 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, així com el compliment de la legislació vigent. Aquests s'agrupen per grups d'accions o procediments operatius orientats a combatre les amenaces a les quals una instal·lació SQL està exposada. 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 *SQL Server.*	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C1. Mantenir actualitzats els servidors amb els service packs i pegats de seguretat publicats per Microsoft. Abans d'instal·lar un nou *service pack* a producció, però, s'ha de testejar a l'entorn de desenvolupament. Es pot conèixer la versió instal·lada actualment executant: `SELECT @@version` 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
C2. En entorns de producció, s'ha d'instal·lar SQL Server en màquines dedicades. S'ha d'evitar fer instal·lacions en controladors de domini o servidors web.	C I D
C3. Assegurar-se que el sistema operatiu del servidor de base de dades acompleix el que proposa la guia de protecció d'entorns Windows (*Guia protecció entorns Windows 2003*).	C I D
C4. Utilitzar particions NTFS per instal·lar SQL Server 2005.	C I
C5. Ubicar en particions separades els fitxers de dades i fitxers de logs de SQL Server.	C I D
C6. Protegir tots els directoris que continguin logs, còpies de seguretat, exportacions de dades o qualsevol altra informació de la base de dades de forma que només tinguin accés els usuaris que ho necessitin. Es pot comprovar quins directoris està utilitzant una base de dades executant l'script: `SELECT filename FROM master.dbo.sysdatabases`	C I
C7. Utilitzar RAID per a bases de dades crítiques. Utilitzar el nivell de RAID que proporcioni la millor fiabilitat i rendiment per a l'entorn (normalment *RAID* 1 o *RAID* 5).	D
C8. Instal·lar només els mòduls de SQL Server 2005 (Analysis Services, Reporting Services, ...) necessaris.	C I D
C9. Inhabilitar tots aquells serveis de SQL Server que no siguin necessaris.	C I D
C10. En servidors amb sistema operatiu Windows, denegar el permís d'execució sobre els arxius dels directoris WINNT o WINDOWS i a system32 per a l'usuari administrador de SQL Server.	C I D
C11. Per entorns SQL Server 2000, desinstal·lar dels entorns de producció les bases de dades d'exemple (Northwind, Pubs, OLTP d'AdventureWorks). Esborrar també dels entorns de producció totes les bases de dades que no siguin necessàries (còpies de bases de dades, versions antigues...). Anar amb compte de no esborrar les bases de dades Master, msdb, model i tempdb.	C I D
C12. Quan s'instal·la SQL Server 7.0, 2000 o MSDE 1.0 o algun dels seus *service packs* queda informació sensible i inclús contrasenyes als logs d'instal·lació: • sqlstp.log • sqlsp.log • setup.iss Esborrar o modificar aquests logs una vegada finalitzada la instal·lació. En SQL Server 2000 es troben a les carpetes: *Arxius de Programa\Microsoft SQL Server\MSSQL\Install* i *Arxius de Programa\Microsoft SQL Server\ MSSQL$<Nom_Instància>\Install folder* En SQL Server 7.0 es guarda una còpia a:	C I D

%SystemDrive%\MSSQL7\Install	
C13. Si el sistema és una actualització de SQL Server 7.0 esborrar els següents fitxers: • *setup.iss* de la carpeta %Windir% (per defecte c:\Windows), • *sqlsp.log* de la carpeta temporal de Windows per contrasenyes.	C I D
C14. Caldrà donar compliment a la *Norma de còpies de seguretat* per a garantir que es realitza còpia de seguretat dels sistemes	C I D
C15. No utilitzar en entorns d'explotació els certificats *SSL* creats per entorns de proves o pre-producció.	D
C16. Si es crea una base de dades de proves o pre-producció a partir d'una altra en producció, tenir en compte la legislació vigent en matèria de protecció de dades.	C I D

Recomanacions

R1. Es recomana no utilitzar els ports per defecte de SQL (1433 i 1434) sinó uns altres d'alternatius.
R2. Es recomana limitar el nom de les instàncies a menys de 16 caràcters sense fer referència a un nombre de versió o altra informació sensible.
R3. Microsoft subministra una eina gratuïta (K*illPwd*) que busca i elimina dels arxius d'instal·lació tots els rastres de contrasenyes (SQL Server 2000). Si s'utilitza amb l'opció /N, mostra la llista de canvis que farà abans de fer-los.
Per SQL Server 2005 aquesta eina encara no es troba disponible.

4.2. CN - Configuració

OBJECTIUS	
Deshabilitar tots els serveis Windows i SQL Server no utilitzats i protegir tots els fitxers i directoris que continguin informació sensible.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C17. Pels usuaris de sistema de SQL Server, utilitzar autenticació Windows en lloc del mode mixt (autenticació Windows i SQL). Pels usuaris d'aplicacions, utilitzar l'autenticació de SQL Server.	C I D

C18. Assegurar que el grup Everyone no te accés a les següents claus del registre de Windows:
`HKEY_LOCAL_MACHINE\Software\Microsoft\MSSQLServer`
`HKEY_LOCAL_MACHINE\Software\Microsoft\MicrosoftSQLServer\InstanceName`
És recomanable, però no obligatori, que els administradors de la màquina tampoc tinguin accés als registres. Els únics usuaris que haurien de poder accedir són el grup *Administradors de Base de Dades*.
	C I D

C19. SQL Server suporta molts protocols de connexió. Deshabilitar tots els que no s'utilitzin (el més utilitzat per les aplicacions és TCP/IP). Es pot fer seleccionant:
`SQL Server Programs`
`Server Network Utility`
	C I D

C20. Per entorns SQL Server 2000, revocar els permisos d'execució del grup *Public* pels següents procediments: sp_OACreate sp_OADestroy sp_OAGetErrorInfo sp_OAGetProperty sp_OASetProperty sp_OAStop sp_OAMethod xp_regread xp_regaddmultistring xp_regdeletekey	C I D

xp_regdeletevalue
xp_regenumkeys
xp_regenumvalues
xp_regremovemultistring
xp_regwrite
xp_regremove
xp_instance_regread
xp_instance_regaddmultistring
xp_instance_regdeletekey
xp_instance_regdeletevalue
xp_instance_regenumkeys
xp_instance_regenumvalues
xp_instance_regremovemultistring
xp_instance_regwrite
xp_instance_regremove
xp_webserver
xp_servicecontrol
xp_availablemedia
xp_dirtree
xp_enumdsn
xp_loginconfig
xp_makecab
xp_ntsec_enumdomains
xp_terminate_process
xp_cmdshell
 	
Per a fer-ho, utilitzar la sentència
`Use master`
`REVOKE EXECUTE ON [procedure] FROM [user]`	

C21. Revocar els permisos d'execució del grup *Public* pels procediments "Database Mail i SQL Mail", si no és necessari enviar correus des del servidor de SQL Server.	C I D
C22. 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
C23. Deshabilitar el protocol de xarxa "Named Pipes". Si es requereix l'ús de "Named Pipes" canviar el nom a qualsevol altre que no sigui \\.\pipe\sql\query.	

Recomanacions

R10. Microsoft SQL Server 2005 pot utilitzar la Capa de sockets segurs (SSL) per a xifrar totes les dades transmeses a través d'una xarxa entre una instància de SQL Server i una aplicació client. El xifrat SSL es realitza en la capa del protocol i està disponible per a tots els clients SQL Server, excepte els clients DB Library i MDAC 2.53.

R11. Assegurar-se que els user-defined stored procedures, són emmagatzemats de forma encriptada, mitjançant la comanda WITH ENCRYPTION en la sentència alter procedure. Utilitzar-ho quan són poques línies, sinó cal realitzar-ho amb alguna eina externa de xifrat.

4.3. MN - Monitoratge

OBJECTIUS	
Registrar tots els intents d'accés a bases de dades SQL Server per tal de poder conduir futures investigacions en cas de necessitat i atribuir-ne responsabilitats.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C24. 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
C25. Pels sistemes d'àmbit departament / ens, es connectaran a eines de correlació de	C I

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.	
C26. 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

Recomanacions

R12. Es recomana, revisar periòdicament les traces per a detectar activitats anòmales que puguin comprometre la seguretat del sistema

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**
C27. Complir les mesures de seguretat indicades a la *Norma contrasenyes* en relació amb la gestió i utilització de contrasenyes d'usuaris.	
C28. No utilitzar mai contrasenyes en blanc. Per verificar que no hi ha contrasenyes en blanc, es pot executar el següent *script*: `select NAME, PASSWORD from master.dbo.SYSLOGINS where PASSWORD is null and NAME is not null`	C I
C29. Definir per l'usuari "*sa*" una contrasenya forta i diferent per a les diferents instal·lacions de SQL Server.	C I
C30. L'usuari "*sa*" no ha de ser utilitzat ni per les aplicacions ni pels usuaris ni pels administradors.	C I
C31. Reanomenar l'usuari "sa" per a evitar atacs sobre l'usuari.	C I
C32. Per entorns SQL Server 2000, deshabilitar (treure permisos de *Connect*) l'usuari *Guest* (l'usuari de la base de dades, no de l'AD) de totes les bases de dades.	C I
C33. Utilitzar diferents comptes d'usuari de Windows per a l'execució de diferents serveis SQL Server.	C I D
C34. Els comptes d'usuari per a cada servei de SQL Server han de ser usuaris locals sense privilegis d'administració. Només s'utilitzaran comptes de domini si el SQL Server ha d'interactuar amb altres sistemes del domini. Aquests comptes hauran de tenir el mínim de privilegis possibles.	C I D
C35. Esborrar els comptes d'usuari no necessaris (això inclou usuaris utilitzats durant les fases de desenvolupament i test de l'aplicació).	C I
C36. Assignar els permisos adequats a les taules, vistes i camps de les mateixes per a cada usuari, i sempre amb els principi de mínims privilegis.	C I
C37. Per entorns SQL Server 2000, especificar contrasenyes per els usuaris *owner* (per evitar que pugui ser modificat) i *user* (per evitar que pugui ser executat) dels paquets DTS.	C I
C38. Per entorns SQL Server 2000, restringir l'accés a les carpetes a on s'emmagatzemen paquets DTS de forma que només en tinguin accés els usuaris autoritzats.	C I
C39. Utilitzar només els rols fixes de servidor sysadmin, serveradmin, setupadmin, etc per a donar suport a l'activitat DBA.	C I
C40. No concedir permisos d'objecte a PUBLIC o GUEST.	C I D
C41. Evitar l'assignació de funcions predefinides a PUBLIC o GUEST.	C I D
C42. No permetre que variables d'entorn, fitxers de text, crides a scripts, etc. continguin usuaris o contrasenyes. Una alternativa és xifrar aquesta informació i desxifrar-la en temps real fent servir algun procediment sobre el qual siguin necessaris certs privilegis.	C I D

Recomanacions

R13.És preferible assignar permisos als rols enlloc d'usuaris directament. D'aquesta manera es facilita el manteniment.

4.5. AU - Auditoria

OBJECTIUS	
Tasques d'auditoria sobre el sistema SQL Server.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C43.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 l'administració de sistemes *SQL Server*.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C44.Es recollirà contractualment el compliment de les normes i guies que el CTTI tingui per l'entorn *SQL Server* així com qualsevol altra norma de gestió o administració que sigui d'aplicació.	C I D
C45.Es garantirà el compliment de la *Norma de contractació de tercers*.	C I D
C46.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 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

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

RAID: *Acrònim de Redundant Array Of Independent/Inexpensive Disks*. És un terme anglès que fa referència a un *conjunt de discos redundants independents/barats*. Aquest tipus de dispositius s'utilitzen para augmentar la integritat de les dades en los discos, millorar la tolerància a errades i millorar el rendiment. En general permeten proveir discos virtuals d'una mida major al dels discos comunament disponibles.

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).

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

SSL: *Secure Socket Layer*. Protocol de comunicacions on es xifra el contingut dels paquets, utilitzat sobretot per comunicar dos punts a través d'una xarxa insegura com Internet.

10 DOCUMENTACIÓ REFERENCIADA

- http://www.microsoft.com
- GE-GUI10 Guia protecció entorns Windows 2003
- GE-GUI19 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
- GE-GUI40 Guia de còpies de seguretat
- NOR-GSEG-070308-v1.0 Norma de gestió de vulnerabilitats de programari base
- SC-NOR16-01 Norma de gestió de traces

11 PARAULES CLAU

Base de dades, usuaris, grups, rols, privilegis, permisos, comunicacions, protocol, administració, pegats de seguretat, SQL Server, protecció, hardening.

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.