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	21/7/2009

Estàndard signat digitalment pel:
Generalitat de Catalunya
Centre de Telecomunicacions i Tecnologies de la Informacio
Estàndard aprovat
Barcelona
2009.07.27 10:52:50 +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 *Oracle*, amb l'objectiu de garantir la confidencialitat, integritat i disponibilitat de la informació i serveis suportats per aquesta plataforma.

ÀMBIT

Bases de dades *Oracle* 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 Oracle.

1 OBJECTIU

Definir els controls per instal·lar, configurar, mantenir i explotar un *SGBD* Oracle 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 Oracle.

Tots els canvis proposats en aquesta guia han de ser primer instal·lats en un entorn de desenvolupament i s'ha de 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 Oracle 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 Oracle. 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 d'Oracle 9i en endavant.

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 Oracle, però no per administrar el sistema en sí.

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 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, 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 un entorn d'aplicacions està exposat. 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 *SGBD* Oracle. Els controls apliquen a entorns de producció.	
CARACTERÍSTIQUES	
Descripció	**Categoria**

C1. Mantenir actualitzat Oracle amb els darrers pegats de seguretat. Pels sistemes ubicats en l'àmbit dels *Serveis TIC Centrals*, cal donar compliment a la *Norma de gestió de vulnerabilitats de programari base*.	I D
C2. Esborrar l'eina *tkprof*, que s'instal·la per defecte, en entorns de producció o, si no és possible, canviar els permisos de manera que només sigui utilitzada pels usuaris que la necessiten. Aquesta eina és un ajut per al desenvolupament i, per tant, no té sentit en entorns de producció.	C I D
C3. Esborrar els fitxers *.dat relacionat amb otrace, del directori <ORACLE_HOME>/otrace/admin si s'ha seleccionat l'eina *Enterprise Manager Grid Controller*, que no s'instal·la per defecte.	C I
C4. Esborrar els objectes de l'*OEM* si no es fan servir. Per fer això, executar <ORACLE_HOME>/rdbms/admin/catnsnmp.sql i esborrar el fitxer <ORACLE_HOME>/bin/dbsnmp.	C I
C5. En servidors amb sistema operatiu Windows, denegar el permís d'execució dels arxius que estan al directori WINNT o WINDOWS i a system32 per a l'usuari administrador d'Oracle.	C I D
C6. Al registre de Windows, donar accés complet a l'usuari d'Oracle a la clau HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE i treure l'accés a la resta d'usuaris, excepte aquells que ho necessitin per algun motiu.	C I D
C7. Al registre de Windows, crear o actualitzar el valor de OSAUTH_PREFIX_DOMAIN en HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\ALL_HOMES posant-ho a TRUE, de manera que en l'autenticació a la base de dades utilitzant usuaris de Windows es tingui en compte també el domini.	C I D
C8. Configurar el *listener.ora* per tal que no faci servir el nom per defecte i que utilitzi adreces IP en comptes de noms de màquines.	C D
C9. No utilitzar el nom o *SID* per defecte per la creació de bases de dades.	C D
C10. No utilitzar en entorns d'explotació els certificats *SSL* creats per entorns de proves o pre-producció.	D
C11. 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
C12. 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, Solaris, AIX, HP-UX, Windows 2003*).	C I D
C13. Col·locar el servidor amb Oracle darrere d'un tallafoc que només permeti l'accés pels ports de servei que ofereix Oracle.	C I D
C14. Si existeix un conjunt de servidors Oracle donant servei (*cluster*), protegir de possibles intrusions les comunicacions privades de replicació entre els servidors.	C I D
C15. 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
C16. Cal netejar la cache abans de parar la base de dades per tal que les seves dades no puguin ser accedides sense autorització.	C I
C17. Els fitxers de control i els registres de reconstrucció de la base de dades (*redo logs*) han d'estar duplicats i guardats en dispositius físicament diferents, per assegurar la disponibilitat de la informació.	I D
C18. No instal·lar Oracle en un controlador de domini de Windows.	C I D
C19. 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
C20. 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. Abans d'instal·lar Oracle, assegurar-se que no hi ha cap usuari connectat al sistema.

R2. Sempre que sigui possible, utilitzar les funcionalitats de seguretat de l'entorn de treball de l'*OEM*.

R3. Els canvis es realitzaran sobre entorns de proves o pre-producció abans d'aplicar-los en entorns d'explotació.
R4. Canviar el port per defecte del *listener.ora*, per tal de reduir el risc d'atac contra el port conegut.
R5. Utilitzar RAID 5 per a reduir el cost sense un impacte significatiu en el rendiment. Per a cassos amb alts requeriments de I/O utilitzar RAID 0+1 quan sigui possible.
Consultar: http://www.oracle-base.com/articles/misc/RAID.php#OracleRAIDUsage

4.2. CN - Configuració

OBJECTIUS	
Configurar la instal·lació del *SGBD* Oracle per a garantir la seguretat dels serveis que presta, així com indicar els requeriments, en alguns casos, dels objectes Oracle que formen les bases de dades.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C21. En general, els fitxers i directoris dintre de <ORACLE_HOME> han de tenir permisos totals només per l'usuari i grup administrador d'Oracle, excepte els fitxers de <ORACLE_HOME>/bin, que han de poder ser llegits i executats per qualsevol usuari.	C I D
C22. En entorns Unix, tots els fitxers en el directori <ORACLE_HOME>/bin han de tenir els permisos activats a 0755 o menys. en els sistemes Unix.	C I D
C23. En entorns Unix, tots els fitxers en el directori <ORACLE_HOME> (excepte per a <ORACLE_HOME>/bin han de tenir permisos activats a 0750 o menys.	C I D
C24. En entorns Unix, assegurar-se que el valor de umask és 022 per al propietari del programari Oracle abans d'instal·lar Oracle.	C I D
C25. Dintre del fitxer init.ora, els fitxers als quals fan referència els paràmetres ifile, control_files i log_archive_dest_n han de ser propietat de l'usuari i grup administrador d'Oracle.	C I D
C26. Dintre del fitxer init.ora, el fitxer al qual fa referència el paràmetre audit_file_dest ha de ser propietat de l'usuari administrador d'Oracle i només aquest ha de tenir permisos de lectura i escriptura.	C I D
C27. Dintre del fitxer init.ora, els directoris als quals fan referència els paràmetres user_dump_dest, background_dump_dest i core_dump_dest han de ser propietat de l'usuari i grup administrador d'Oracle.	C I D
C28. Dintre del fitxer init.ora, verificar que el paràmetre trace_files_public està a FALSE, ja que així els usuaris no poden llegir els fitxers de traces	C
C29. Dintre del fitxer init.ora, posar a TRUE el paràmetre global_names per tal que Oracle comprovi que el nom d'un enllaç a una base de dades és el mateix que la base de dades remota.	C I D
C30. Dintre del fitxer init.ora, verificar que el paràmetre remote_os_authent té el valor FALSE, de manera que obligatòriament sigui necessari introduir una contrasenya per accedir a la base de dades i no s'utilitzi un usuari del sistema operatiu per autenticar-se a la base de dades.	C I D
C31. Dintre del fitxer init.ora, verificar que el paràmetre remote_os_roles té el valor FALSE, per tal que els usuaris remots no es puguin autenticar com usuaris amb rols o grups del sistema operatiu local.	C I D
C32. Dintre del fitxer init.ora, verificar que el paràmetre os_roles té el valor FALSE per tal de distingir entre l'administrador del sistema i l'administrador de la base de dades.	C I D
C33. Dintre del fitxer init.ora, canviar el paràmetre audit_trail, posant-li el valor OS, que és el requerit quan l'auditor és una persona diferent de l'administrador de la base de dades.	C I
C34. Dintre del fitxer init.ora, el paràmetre os_authent_prefix ha de ser una cadena diferent de OPS$ (que és el valor per defecte). Especificar un valor "" (null).	C
C35. Dintre del fitxer init.ora, el paràmetre sql92_security ha d'estar a TRUE per assegurar que els usuaris hagin de tenir privilegis de SELECT sobre una taula per executar les comandes UPDATE i DELETE utilitzant clàusules WHERE sobre aquesta taula.	C I D
C36. Dintre del fitxer init.ora, posar el paràmetre os_dictionary_accessibility a FALSE per	C

tal que un usuari amb privilegis de SELECT sobre qualsevol taula no pugui veure el diccionari.	
C37. Dintre del fitxer init.ora, esborrar la línia dispatcher=(PROTOCOL=TCP)(SERVICE=<oracle_sid>XDB) per deshabilitar els ports ftp 2100 i http 8080, els quals es configuren en la instal·lació predeterminada d'inici amb Oracle 9iR2. Per defecte està configurat en el spfile en 9i i 10g.	C I D
C38. Dintre del fitxer init.ora, canviar el paràmetre audit_sys_operations a TRUE per auditar les activitats dels usuaris autenticats com SYSDBA o SYSOPER.	C I D
C39. Dintre del fitxer sqlnet.ora, posar a YES el paràmetre tcp.validnode_checking i indicar les adreces IP dels servidors autoritzats amb el paràmetre tcp.invited_nodes o bé indicar les adreces dels no autoritzats amb el paràmetre tcp.excluded_nodes. Això permetrà limitar els clients als quals contestarà el *listener* davant una petició.	C D
C40. Dintre del fitxer sqlnet.ora, configurar sqlnet.inbound_connect_timeout i sqlnet.expire_time amb uns valors petits inicialment (per exemple 3 i 10 respectivament) i anar augmentant-los segons sigui necessari.	C D
C41. En Oracle 9i, esborrar el fitxer executable <ORACLE_HOME>/bin/extproc si no es fa servir i la seva referència des dels fitxers tnsnames.ora i listener.ora. Si s'utilitzés el binari *extproc*, consultar com aplicar les mesures de seguretat pertinents al *Metalink Security Alert* 57 (244523.1) d'Oracle.	C I D
C42. Crear un *listener* específic per l'administració d'Oracle i protegir-lo amb mecanismes de xifrat de comunicacions (*SSL*).	C I D
C43. Establir una contrasenya xifrada per al *listener*. Per defecte la contrasenya del *listener* no està activada (en 9i).	C D
C44. En cas de necessitar xifrar la transmissió i/o emmagatzemament de dades (requeriments legals o de seguretat), implementar la funcionalitat del mòdul *OAS (Oracle Advanced Security)* per a versions 10gR2 o superiors. Per a versions inferiors, utilitzar el paquet DBMS_OBFUSCATION_TOOLKIT. Utilitzar només el xifrat amb els algorismes disponibles a *OAS* si no es possible fer-ho per *SS*L (dependrà dels clients que es connecten a la base de dades). NOTA: En cas d'activar *OAS*, cal donar compliment als requeriments recollits a l'apartat "Configuració OAS".	C I
C45. En cas d'instal·lar un certificat de servidor, establir el fitxer tnsnames per a incloure el paràmetre SSL_SERVER_CERT_DN amb el nom distingit (DN) del certificat.	C I
C46. En cas d'utilitzar un procediment PL/SQL que inclogui el paquet DBMS_OBFUSCATION_TOOLKIT, que permet xifrar dades d'una taula, tenir en compte que la crida al procediment de xifrat i desxifrat necessita com paràmetre la clau de xifrat. Per tant, aquesta ha de ser emmagatzemada per la seva posterior utilització. L'emmagatzemament de la clau de xifrat s'ha de fer de manera segura i evitant l'accés no autoritzat a la mateixa.	C
C47. En cas que es faci un xifrat de les dades d'una taula, incloure almenys una dada identificativa del registre a l'algorisme de xifrat, així no hi hauran registres xifrats de la mateixa manera i es reduirà el risc de desxifrar el contingut per inducció.	C
C48. Treure el privilegi d'execució per a tots els usuaris del procediment DBMS_OBFUSCATION_TOOLKIT, que podria permetre desxifrar dades.	C I
C49. 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

R6. El DBMS_OBFUSCATION_TOOLKIT ha estat reemplaçat amb el paquet DBMS_CRYPTO, però el DBMS_OBFUSCATION_TOOLKIT es encara necessari per a algunes tasques que no estan disponibles en el paquet DBMS_CRYPTO.

R7. Quan sigui necessari, utilitzar *OLS (Oracle Label Security)*, que permet protegir les dades confidencials o restringides d'accessos no autoritzats. Abans d'implementar *OLS*, cal tenir una còpia de seguretat de les dades a tractar.

Configuració OAS (Oracle Advanced Security)

- El paràmetre sqlnet.encryption_server ha d'estar a REQUIRED per tal de fer obligatòria la comunicació xifrada independentment de la configuració del client. L'algorisme de xifrat s'especifica amb el paràmetre sqlnet.encryption_types_server i caldria que utilitzés una clau d'almenys 128 bits de llargària.
- Assignar el paràmetre sqlnet.crypto_seed amb la llargària màxima de 70 caràcters.
- Per a comprovar la integritat de les dades transmeses entre el client i el servidor, els paràmetres sqlnet.crypto_checksum_server i sqlnet.crypto_checksum_client han de ser REQUIRED i sqlnet.crypto_checksum_types_server ha de ser SHA1.
- Sempre que sigui possible (dependrà de la compatibilitat amb els clients), donar el valor SSL_RSA_WITH_3DES_EDE_CBC_SHA al paràmetre ssl_cipher_suites.
- Posar el paràmetre ssl_version com 3.0, no activar aquest paràmetre amb el valor ANY
- Eliminar les Autoritats de Certificació (CAs) que no siguin requerides.

4.3. MN - Monitoratge

OBJECTIUS	
Registrar tots els intents d'accés a bases de dades Oracle per tal de poder conduir futures investigacions en cas de necessitat i atribuir-ne responsabilitats.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C50. 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
C51. 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
C52. 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

R10. 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	
Identificar i autenticar correctament als usuaris que accedeixen a una base de dades Oracle.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C53. Assignar els privilegis a usuaris amb el mínim accés necessari als objectes de les bases de dades (taules, vistes i camps) i revocar els privilegis quan ja no siguin necessaris.	C I D
C54. Executar els serveis d'Oracle usant un compte d'administrador local creada específicament per a Oracle. Usar el compte creat per a instal·lar el producte.	C I D
C55. Denegar l'inici de sessió de l'usuari administrador d'Oracle.	C I D
C56. L'usuari administrador d'Oracle no ha de pertànyer al grup o a un dels grups d'administradors del sistema.	C I D
C57. Només els usuaris que ho requereixin han de pertànyer al grup de l'administrador d'Oracle.	C I D
C58. No escriure comandes ni scripts que continguin contrasenyes en utilitzar l'*OEM* en mode de línia de comandes, ja que es podrien llegir si algun usuari visualitza els processos del sistema.	C I D

C59. No s'ha de permetre l'execució de scripts que generin processos on usuaris o contrasenyes siguin visibles en la llista de processos del sistema.	C I D
C60. 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
C61. Els enllaços entre bases de dades no poden contenir usuaris i contrasenyes escrits al mateix codi.	C I D
C62. Complir les mesures de seguretat indicades a la *Norma de contrasenyes* en relació amb la gestió i utilització de contrasenyes d'usuaris.	C I D
C63. No tenir bases de dades de producció juntament amb les de proves o pre-producció.	C I D

4.5. AU - Auditoria

OBJECTIUS	
Tasques d'auditoria sobre el sistema Oracle.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C64. 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 *Oracle*.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C65. Es recollirà contractualment el compliment de les normes i guies que el CTTI tingui per l'entorn *Oracle* així com qualsevol altra norma de gestió o administració que sigui d'aplicació.	C I D
C66. Es garantirà el compliment de la *Norma de contractació de tercers*.	C I D
C67. 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

DWH: *Data Warehouse*. Tipus de base de dades relacional amb informació relativa al negoci d'una organització, que s'obté generalment extraient dades d'altres bases de dades.

Listener: És el procés que rep les peticions de consultes a bases de dades i hi accedeix per extreure la informació i servir-la.

OAS: *Oracle Advanced Security*. És mòdul addicional d'*Oracle Enterprise Edition* que serveix per implementar mesures de seguretat específiques, tals com comprovació de la integritat de dades transmeses entre el client i el servidor Oracle i el xifrat d'aquestes.

OEM: *Oracle Enterprise Manager*. Consola d'administració del SGBD Oracle.

OLS: *Oracle Label Security*. És mòdul addicional d'*Oracle Enterprise Edition* que serveix per implementar mesures de seguretat a nivell de taula i de files dintre les taules.

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.

SGBD: Sistema Gestor de la Base de Dades. És el programari que s'encarrega de gestionar els accessos dels usuaris a les dades que necessiten.

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).

SID: *System Identification*. Cadena de caràcters amb que s'identifica una base de dades per distingir-la de les altres.

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

- GE-GUI07 Guia protecció entorns Linux
- GE-GUI08 Guia protecció entorns Solaris
- GE-GUI10 Guia protecció entorns Windows 2003
- GE-GUI27 Guia protecció entorns HP-UX
- GE-GUI32 Guia protecció entorns AIX
- 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
- NOR-GSEG-070308-v1.0 Norma de gestió de vulnerabilitats de programari base
- GE-GUI40 Guia de còpies de seguretat
- SC-NOR16-01 Norma de gestió de traces

- Documentació
  - Pegats de seguretat: http://metalink.oracle.com/metalink/plsql/ml2_gui.startup
  - *Oracle Net Services*: http://www.psoug.org/reference/net_services.html
  - *Oracle Product Security*: http://www.oracle.com/technology/deploy/security/nissc00.htm
  - *Oracle Metalink:* https://metalink.oracle.com
  - *Oracle Advanced Security:* http://www.oracle.com/technology/deploy/security/database-security/advanced-security/index.html
  - *Oracle Label Security:* http://www.oracle.com/technology/deploy/security/database-security/label-security/index.html
  - *Oracle Database Security Checklist:* http://www.databasesecurity.com/oracle/twp_security_checklist_db_database.pdf

11 PARAULES CLAU

Base de dades, usuaris, rols, privilegis, permisos, taula, procediment, xifrat, comunicacions, protocol, tallafocs, Oracle, hardening, 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.