Análisis de seguridad en base de datos: Aplicación Oracle versión 11g

Guillermo Cifuentes Garzón,

Unidad de Gestión de Postgrados;
Escuela Politécnica del Ejército,
Sangolquí, Ecuador
guillogps@gmail.com

RESUMEN: La información es un activo de las organizaciones, permite la toma de decisiones oportunas a nivel gerencial y por consiguiente un alto nivel de competitividad dentro del mercado.Las tecnologías de la información constituyen otro factor determinante para el manejo de la información en las empresas, cuyo mayor o menor grado de automatización genera el nivel de dependencia de la organización con la tecnología, siendo las bases de datos el medio en el cual se almacena y gestiona la información.La Seguridad de la Información ha tomado un lugar determinante en la gestión de la Tecnología de la Información (TI), y se ha convertido en un elemento fundamental para toda estrategia empresarial con miras a lograr metas importantes a corto, mediano y largo plazo con el objetivo de proteger y asegurar la información, considerando las propiedades que son la disponibilidad, integridad y confidencialidad. Si en realidad se pueden definir niveles de seguridad de acuerdo a los estándares y mejores prácticas, con la cual se podrá evidenciar que al aplicarlos se reduce el riesgo de intrusiones a la base de datos. El presente articulo sedcribe un checklist de seguridades que sirven de guia para administradores de base de datos.

PALABRAS CLAVES: Normas, estandares, seguridad, planeaciòn checklist.

ABSTRACT: Information is an asset of organizations , it allows timely decision making at the management level and therefore a high level of competitiveness in the Business.Information tecnologies are determinant factor on information management in Organizations whose has tecnology automatization dependency, therefore the information is stored in databses and their security is important. Data security has taken a leading place in the management information Technology (iT) , and has become an essential element of any business strategy to achieve important goals in the short, medium and long term in order to protect and secure the information , considering the properties that are the availability , integrity and confidentiality . This article describes a checklist of securities parameters that serve as a guidelines for database administrators.

KEYWORDS: Certification, Audit, Organizational structure, increasing awareness.

1. INTRODUCCIÓN

La información es un activo de las organizaciones, permite la toma de decisiones oportunas a nivel gerencial y por consiguiente un alto nivel de competitividad dentro del mercado.

Las tecnologías de la información constituyen otro factor determinante para el manejo de la información en las empresas, cuyo mayor o menor grado de automatización genera el nivel de dependencia de la organización con la tecnología, siendo las bases de datos el medio en el cual se almacena y gestiona la información.

La Seguridad de la Información ha tomado un lugar determinante en la gestión de la Tecnología de la Información (TI), y se ha convertido en un elemento fundamental para toda estrategia empresarial con miras a lograr metas importantes a corto, mediano y largo plazo con el objetivo de proteger y asegurar la información, considerando las propiedades que son la disponibilidad, integridad y confidencialidad.

En este entorno, la base de datos Oracle es una de las herramientas tecnológicas utilizada principalmente por empresas grandes para el manejo de la información, desde la versión 9i ya incluye aspectos de seguridad como: Label security y Fine grained Auditing[1] . En la versión 10 mejoraron aspectos de seguridad e incluyó nuevos conceptos como: Client identity Propagation[2], Secure configuration scanning[3] , entre otros. Con el paso del tiempo la importancia de la seguridad fue creciendo, por lo que la versión 11g de Oracle incluye: Data Base Vault[4] , Audit Vault[5] , también se protege el flujo de información con Data Masking así como también con Data Encryption. Esta versión también tiene un complemento de seguridad que implementa una barrera de firewall propio de Oracle. A pesar de contar con todos estos complementos de seguridad, no define niveles de seguridad para la información almacenada en la base de datos.

El presente proyecto busca definir configuraciones por niveles de seguridad de acuerdo a los estándares y mejores prácticas, con la cual se podrá evidenciar que al aplicarlos se reduce el riesgo de intrusiones a la base de datos. La Tesis es una guía para administradores de Base de Datos que requieran implementar niveles de seguridad en Oracle11g.

II. Metodología

La metodología usada es la deductiva. Primero se estudiaron las buenas prácticas, normas internacionales como la ISO 27000 y estándares existentes para poder crear un checklist con características de seguridad que se pueden aplicar a la base de datos Oracle 11g

[1] Fine grained Auditing: (FGA) Permite que las políticas de auditoria puedan ser asociadas con columnas específicas de las tablas de la aplicación.

[2] Client identity Propagation: Permite a un cliente actuar como un agente de otro cliente usando la identidad del cliente original.

[3] Secure configuration scanning: Característica de seguridad que monitorea la configuración de seguridad.

[4] Data Base Vault: Centraliza los controles de seguridad en el denominado baúl.

[5] Audit Vault: Centraliza las políticas y controles de auditoria en el denominado baúl.

III. Evaluación de resultados y discusión

El resultado del análisis se resume en un checklist con las características de seguridad esenciales y avanzadas identificadas para mejorar la seguridad en la base de datos Oracle.

Los niveles de seguridad y colores definidos para la lista de verificación del proyecto, son los siguientes:

- Bajo (1) 
- Medio (2) 
- Alto (3) 

Estos niveles son determinados de acuerdo al siguiente criterio:

Nivel 1 (Bajo).- El nivel bajo es considerado el nivel más básico de configuraciones de seguridad que deben estar implementadas en un ambiente de base de datos Oracle. Muchas de estas configuraciones básicas vienen activadas por defecto y dependiendo del enfoque de la organización se refuerzan o desactivan.

Nivel 2 (Medio).- El nivel medio es un ajuste personalizado a parámetros de seguridad específicos en la base de datos con el que se refuerza la seguridad de la misma y convierte a la base de datos en un elemento seguro.

Nivel 3 (Alto).- El nivel alto como su nombre lo indica es un nivel superior de seguridad, en el que no solo se refuerzan las características de seguridad sino que se monitorea las actividades en la base de datos para poder encontrar cualquier anomalía, acceso no autorizado e intrusión en la base de datos. Este nivel al ser el más complejo y abarcar a los otros dos es a menudo usado por entidades financieras, gubernamentales, y cualquier otra que quiera invertir en la seguridad de su información.

Tabla. Check list seguridades en Oracle

	Nivel de seguridad	O/S	Observación/Configuración
PLANEACIÓN Y EVALUACIÓN DE RIESGOS			
Revisar las versiones y gestionar los parches de Oracle	2	Todos	SQL> select * from v$version;

Configurar Backups periódicos de la base de datos	1		Todos	
Guardar el archivo SPFILE y CONTROLFILE en un lugar seguro y respaldar una copia de los mismos	3		Todos	RMAN> CONFIGURE CONTROLFILE AUTOBACKUP ON;
Revisar Políticas y procedimientos de la Base de datos	2		Todos	
Sistema operativo y aspectos de seguridad				
Revisar los permisos del propietario de la carpeta $ORACLE_HOME/bin	2		Linux, Unix	$ ls –l
Bloquear la cuenta por defecto del software de Oracle	1		Todos	SQL> alter user oracle account block;
Revisar permisos del archivo de trace	2		Linux, Unix	$ ls –l
Revisar permisos de los Data files	1		Linux, Unix	$ ls –l
Auditar scripts que contengan usuarios y contraseñas	3		Todos	
Auditar los archivos de configuración de los clientes que contengan usuarios y contraseñas	3		Todos	
Guardar los logs en un servidor distinto	2		Todos	
Asegurarse que ningún usuario tenga privilegios de ALTER SESSION y ALTER SYSTEM	1		Todos	SQL> select * from dba_sys_privs where privilege =`ALTER SESSION'; SQL> revoke alter session to <user>;
AUTENTICACIÒN				
Auditar actividades de usuarios	3		Todos	
Auditar logins de la base de datos de aplicación.	3		Todos	SQL> ALTER SYSTEM SET audit_trail = "DB” SCOPE=SPFILE;
Auditar las contraseñas de los usuarios de la base de datos	3		Todos	
CONTROLES DE ACCESO				

Asegurar la vista ALL_USERS	2		Todos	SQL> select * from all_tab_privs_made;
Asegurar acceso al catálogo de roles	3		Todos	Permisos en la vista role_role_privs
Asegurar acceso a las vistas del rol dba	3		Todos	
Crear un rol para gestionar las cuentas de usuario	2		Todos	
Revisar que el parámetro log_archive_start este activado	2		Todos	SQL> alter system archive log start;
Revisar que el parámetro os_authent_prefix este en NULL	1		Todos	SQL> alter system set os_authent_prefix='' scope=spfile sid='*';
Revisar el parámetro O7_dictionary_accessibility este desactivado	1		Todos	SQL> show parameter O7_dictionary_accessibility;
Revisar el parámetro *remote_os_authent* este desactivado	3		Todos	SQL> show parameter remote_os_authent;
Revisar que el parámetro *remote_listener* este en NULL	1		Todos	SQL> alter system set remote_listener='';
Revisar usuarios que tengan el privilegio de *dba*	2		Todos	SQL> select * from DBA_ROLES;
Revisar que no exista usuarios o roles con todos los privilegios asignados	1		Todos	
Revisar los accesos directos otorgados a objetos o tablas	2		Todos	
Revisar usuarios con el privilegio *BECOME_USER*	1		Todos	
Revocar el privilegio *public execute* en el archivo *utl_file*	1		Todos	SQL> revoke execute on utl_file from public;
Revocar el privilegio *public execute* en el archivo *utl_tcp*	1		Todos	SQL> revoke execute on utl_tcp from public;
Revocar el privilegio *public execute* en el archivo *utl_http*	1		Todos	SQL> revoke execute on utl_http from public;

Revocar todos los permisos no necesarios del rol *PUBLIC*	3		Todos	SQL> revoke create view from PUBLIC;
Setear el tiempo de vida de las contraseñas a 60 días	2		Todos	SQL> create profile all_users limit PASSWORD_LIFE_TIME 60;
Setear el intento de login a 5	2		Todos	SQL> alter profile all_users set failed_login_attempts = 5;
Setear el re-uso de contraseña a máximo 2	3		Todos	SQL> alter profile all_users set PASSWORD_REUSE_TIME= 2;
Auditar los triggers de los usuarios	2		Todos	
RED				
Auditar el archivo *listener.ora*	3		Todos	
Forzar al despachador MTS a usar puertos específicos	3		Todos	
No usar los puertos del listener por defecto 1521 1526	2		Todos	Modificar el listener.ora
No usar nombres de servicio conocidos Ej; ORCL	2		Todos	
Usar Oracle advance security para encryptar transmisión de datos	3		Todos	
Deshabilitar puertos de Oracle que no sean necesarios	3		Todos	
DISPONIBILIDAD BACKUP Y RECOVERY				
Asegurarse que la base este en modo *ARCHIVE LOG*	2		Todos	SQL>alter database ARCHIVELOG;
Revisar los backups regularmente	1		Todos	
Guardar los backups en discos diferentes al de la data y si es posible en cinta	3		Todos	

2. TRABAJOS RELACIONADOS

Con respecto a investigacion o analisis de seguridad en base de datos es reducido, ya que solo companias especializadas realizan estas pruebas para poder desarrollar software propietario que atienda esta necesidad de protección de la informacion.

También existen trabajos relacionados con automatizar la toma de informaciòn de auditoria para poder analizarla de mejor manera y tomar decisiones mas oportunas.

3. CONCLUSIONES Y TRABAJOS FUTUROS

Debido a varias estafas y fraudes hoy en día existen normas y estándares que se exigen a ciertas organizaciones, Oracle dentro de su manejador de base de datos cumple con varias de estas regulaciones para facilitar a las empresas que usan esta base de datos el cumplimiento regulatorio.

El análisis de la información obtenida acerca de las normas o estándares de base de datos nos muestra que no existe una guía especializada en seguridad de base de datos Oracle con parámetros específicos.

Los niveles de seguridad obtenidos en este proyecto sirven como referencia para administradores de base de datos Oracle que quieran implementar o mejorar sus seguridades.

En el mundo globalizado la complejidad de la tecnología va aumentando por lo que si se quiere proteger la información, se debe tener personal capacitado lo cual debe ser tomado en cuenta en el presupuesto del área de tecnología.

Los complementos de seguridad para la base de datos Oracle pueden ser un problema por su costo, pero dependiendo de la planificación en el presupuesto, la importancia que se le de a resguardar la información y al costo beneficio que se obtenga al darle valor a la información puede justificarse la inversión en seguridad.

4. AGRADECIMIENTOS

Ofrezco agradecimientos a mi tutora, la Ingeniera Nancy Velásquez por su dedicación y sabiduría, también agradezco a la Ingeniera Lorena Duque por su apoyo en la culminación de este proyecto.

5. REFERENCIAS BIBLIOGRÁFICAS

- Marlene Theriault, Aaron Newman, Manual de seguridad Oracle 2007 McGraw Hill.

- Jeffrey Wheatman, Marzo 2012. Actividades de la base de datos que se deberían monitorear según Gartner http://www.gartner.com/technology/reprints.do?id=1-1BUG731&ct=120827&st=sb#
- Kevin Sheehan, Base de datos Oracle 11G hardening http://www.securedba.com/securedba/2007/12/hardening-the-o.html#tpe-action-resize-446
- Estadísticas Imperva. http://www.imperva.com/company/company.html
- Jeffrey Wheatman, Febrero 2012. Evolución de monitoreo hacia auditoria y protección. http://www.gartner.com/technology/reprints.do?id=1-1A6PX24&ct=120419&st=sb#
- Segu Info, Junio 2012. Herramientas gratuitas para penetration testing http://blog.segu info.com.ar/2012/06/herramientas-gratuitas-para-penetration.html#axzz2dHCVG1pt