

ACTIVIDAD 4

SEGURIDAD BD

Estudiante: Daniel Vargas Rios

Considere que la aplicación web de un Banco tiene la Base de Datos Oracle. Qué aspectos de seguridad mínimos usted consideraría en la revisión de Base de Datos? (desarrolle a criterio). Para ello considere un PT (Plan de Trabajo) sugerido para esta revisión.

Desarrollando los aspectos de seguridad en una base de datos Oracle, quise aplicar un PT diferente al que se nos fue facilitado en clase, por ello me guie en base a la norma ISO 27000.

Quiero agregar que 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.

Analizando e investigando las normas o estándares de base de datos pudo mostrar que no existe una guía especializada en seguridad de base de datos Oracle con parámetros específicos. 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.

EVALUACION	OBSERVACION
Revisar las versiones y gestionar los parches de Oracle	SQL> select * from v\$version;
Configurar Backups periódicos de la base de datos	
Guardar el archivo SPFILE y CONTROLFILE en un lugar seguro y respaldar una copia de los mismos	RMAN> CONFIGURE CONTROLFILE AUTOBACKUP ON;
Bloquear la cuenta por defecto del software de Oracle	SQL> alter user oracle account block;
Auditar scripts que contengan usuarios y contraseñas	

Asegurarse que ningún usuario tenga privilegios de ALTER SESSION y ALTER SYSTEM	SQL> select * from dba_sys_privs where privilege = `ALTER SESSION`; SQL> revoke alter session to <user>;
Auditar logins de la base de datos de aplicación.	SQL> ALTER SYSTEM SET audit_trail = "DB" SCOPE=SPFILE;
Revisar los accesos directos otorgados a objetos o tablas	
Revisar usuarios con el privilegio BECOME_USER	
Setear el tiempo de vida de las contraseñas a 30 días	SQL> create profile all_users limit PASSWORD_LIFE_TIME 30;
Setear el intento de login a 3	SQL> alter profile all_users set failed_login_attempts = 3;
Setear el re-uso de contraseña a máximo 3	SQL> alter profile all_users set PASSWORD_REUSE_TIME= 2;
No usar nombres de servicio conocidos Ej; ORCL	
Usar Oracle advance security para encryptar transmisión de datos	
Deshabilitar puertos de Oracle que no sean necesarios	
Revisar los backups regularmente	

Existen programas para proteger nuestra base de datos, una que recomiendo es Oracle Data Safe, leyendo sus reseñas y características lo veo una buena opción.