Luis Javier Romero, Ignacio Ochoa, Samuel Núñez, Víctor Sánchez, Pablo Ruiz, Jaime Ruiz

ANÁLISIS DE RIESGOS

Identificación y eliminación de vulnerabilidades de contraseñas:

- A lo largo del proyecto al realizarlo en la máquina virtual hemos empleado la misma contraseña "Oracle" para todas las conexiones y bases de datos lo que supone una importante vulnerabilidad dado a que cualquiera que posea la contraseña de una posee la contraseña de todas. A esto se le suma la baja complejidad de la contraseña empleada lo que la hace vulnerable a ataque de fuerza bruta entre otras.
- **Solución**: Modificar las contraseñas empleando unas generadas aleatoriamente y de suficiente complejidad además de emplear distintas para cada relación. Para ello nos hemos asegurado de que se cumplan los siguiente parámetros:
  - ❖ La contraseña debe ser distinta del nombre de usuario
  - ❖ Las contraseñas deben ser una mezcla de letras, caracteres y números
  - ❖ Las contraseñas deben ser de longitud suficiente
  - ❖ Las contraseñas deben no adivinarse fácilmente

Privilegios de las bases de datos y acceso al control:

- Las mejores prácticas de seguridad dictan que las organizaciones otorguen a las personas los privilegios mínimos necesarios para realizar las funciones laborales requeridas. Los privilegios se pueden usar para acceder a información confidencial cuando a un usuario (o aplicación) se le otorgan derechos de base de datos que exceden estos requisitos.
- A lo largo del proyecto hemos creado vistas y roles para asegurarnos de que se cumple el criterio de confidencialidad entre esquemas externos. De esta forma nos hemos asegurado de que ningún usuario pueda ejercer funciones DDL y hemos permitido a algunos (generalmente de alto nivel) la posibilidad de implementar comandos de DML como inserts.
- En el proyecto no hemos permitido que ningún usuario tenga permisos de DBA lo que reduce el riesgo de modificaciones accidentales de las bases de datos.

Permisos del sistema operativo y conexión red:

- El proyecto ha sido realizado en una máquina virtual que emplea sistema operativo Linux. El realizarlo en una maquina virtual y no desde nuestras máquinas personales permite restringir los permisos que otorgamos al sistema operativo y permite al estar desconectado de la red evitar una serie de riesgos.

Otras medidas:

- De ser un proyecto de mayor duración se podría implementar parches que corrijan brechas de seguridad y defectos a la hora de otorgar permisos a los usuarios.