## SEGURIDAD

Se enumeran aspectos a tener en cuenta para mantener la seguridad e integridad de los datos en la BD; se toma como modelo:

* Las consultas únicas se realizan vía web.
* La BD del sistema instalado en sitio cliente, se actualiza vía Internet.

Para la parte de consultas únicas, se tiene una BD que es consultada por un servicio web, por lo tanto la misma debe estar aislada de Internet.

* Las consultas realizadas por formulario web deberán ser cifradas antes de ser enviadas al servidor; de manera similar serán tratadas la información de respuesta a consultas (Encriptación MD5).
* La BD debe estar alojada en un servidor en una zona desmilitarizada; el firewall debe bloquear el puerto 3306. Se puede comprobar haciendo telnet al servidor con ese puerto.
* No almacenar claves sin cifrar en la BD (tabla usuarios).
* Verificar que los permisos de usuarios sean los mínimos requeridos (Comando SHOW GRANTS).
* Utilizar comillas simples en las constantes numéricas para evitar ejecución de comandos por parte de los usuarios (Comprobar errores ingresando comillas simples y dobles; comprobar todos los valores que se pasan).
* No utilizar usuario de administración para la aplicación.
* Caracteres de escape para caracteres especiales (Pendiente).

Referido a la aplicación que se instala en sitio cliente, se debe tener en cuenta que la BD será actualizada en forma remota. Dependiendo de la infraestructura del cliente (analizar si se necesita requerir algún tipo de topología y seguridad de red para la instalación de los datos, símil características de instalación del server principal), se puede solicitar que se bloquee el acceso externo a la BD de no ser necesario actualizar; esto último responde al modelo de actualizaciones esporádicas (semanalmente o mensualmente).

* Todos los usuarios deben tener clave
* No ejecutar servidor de BD con usuario de root, generar un usuario propio para la BD.
* Privilegios PROCESS, SUPER, FILE sólo para usuarios administrativos.
* Establecer límite de conexiones por cuenta.
* Activar –safe-user-create para evitar que los usuarios sin privilegios de INSERT en la tabla de Usuarios pueda crear nuevos usuarios con GRANT.
* Activar –skip-name-resolver para evitar resoluciones erróneas o maliciosas de nombres de servidores; se guardarán las IPs directamente en las tablas.
* “--skip-networking” deshabilita las conexiones vía TCP/IP a la BD, la misma se hace a través de ficheros sockets en UNIX (Investigar más a fondo para ver si aplica).
* Restringir el permiso SHOW DATABASE a usuarios administrativos.

## ACTUALIZACION

## FUENTE

* <http://dev.mysql.com/doc/refman/5.0/es/security-guidelines.html>
* <http://dev.mysql.com/doc/refman/5.0/es/security-against-attack.html>
* <http://dev.mysql.com/doc/refman/5.0/es/privileges-options.html>
* <http://dev.mysql.com/doc/refman/5.0/es/load-data-local.html>