

Seguridad gestión de grupos y de usuarios

En el apartado seguridad, del menu herramientas, nos encontramos con estos tres apartados:

- **Establecer Contraseña de la base de datos**
- **Permisos de Usuario y Grupos**
- **Cuentas de Usuario y Grupos**

La seguridad en Access puede ser a nivel de archivo o a nivel de sesion. En el primer caso, se protege solo la apertura de una base de datos, archivo mdb o mde de Access. En el segundo caso, la proteccion se amplia a la apertura de una sesion de Access independientemente del fichero mdb o mde que se quiera utilizar.

Veamos ahora como se crea y como se elimina, una contraseña a nivel de archivo.

Establecer Contraseña de la base de datos (Menú Herramientas, Seguridad)

Para asignar una contraseña a una base de datos de Access deberemos seguir los siguientes pasos, teniendo en cuenta que esta contraseña solo es para una base de datos en concreto y que distingue entre mayusculas y minusculas.

1. En el menú **Archivo**, clic en **Abrir**.
2. Clic en la flecha situada a la derecha del botón **Abrir**, a continuación en **Abrir en modo exclusivo**, y por último abra la base de datos.
3. En el menú **Herramientas**, selecciona **Seguridad** y después haga clic en **Establecer contraseña de la base de datos**.
4. Escribe la contraseña y confirma la misma.
5. Haz clic en **Aceptar**.
6. A partir de este momento, la próxima vez que quieras abrir esta base de datos, Access solicitara la contraseña en este archivo.

Quitar una contraseña de base de datos (Menú Herramientas, Seguridad)

1. En el menú **Archivo**, clic en **Abrir**.
2. Clic en la flecha situada a la derecha del botón **Abrir**, a continuación en **Abrir en modo exclusivo**, y por último abre la base de datos.
3. En el cuadro de diálogo **Solicitud de contraseña**, escriba la contraseña de la base de datos y haz clic en **Aceptar**. *Las contraseñas distinguen mayúsculas de minúsculas*
4. En el menú **Herramientas**, selecciona **Seguridad** y después haz clic en **Anular la contraseña establecida para la base de datos**. *Este comando sólo está disponible si anteriormente fue habilitada la contraseña de la base de datos.*
5. En el cuadro de diálogo **Anular la contraseña establecida para la base de datos**, escriba su contraseña actual. (Si esta opción se deja en blanco, habremos quitado la contraseña).
6. Haga clic en **Aceptar**.

Veamos ahora como se define la seguridad a nivel de sesión, cuentas de grupos de trabajo y cuentas de usuarios.

Un poquito de teoría:

La seguridad en Access contiene las siguientes cuentas predefinidas.

Cuenta	Función
Administrador	La cuenta de usuario predeterminada. Esta cuenta es exactamente la misma para cada copia de Microsoft Access y otras aplicaciones que utilicen el motor de base de datos Microsoft Jet, tales como Visual Basic para aplicaciones y Microsoft Excel.
Administradores	El grupo de cuentas del administrador. Esta cuenta es única para cada archivo de información de grupo de trabajo. Está predeterminado que el usuario Administrador pertenezca al grupo Administradores. Como mínimo, deberá haber un usuario en el grupo Administradores en todo momento.
Usuarios	La cuenta de grupo que comprende todas las cuentas de usuarios. Cuando un miembro del grupo Administradores crea una cuenta de usuario, Access agrega la misma al grupo de Usuarios de forma automática. La cuenta es la misma para cualquier archivo de información de grupo de trabajo, pero únicamente contiene las cuentas de usuario creadas por los miembros del grupo de Administradores del grupo de trabajo en cuestión. De forma predeterminada esta cuenta dispone de permisos plenos sobre todos los objetos de nueva creación. La única forma de eliminar una cuenta de usuario del grupo Usuarios es que un miembro del grupo Administradores elimine del grupo al usuario.

De hecho, la seguridad en Access siempre está activada. Hasta el momento en el que se activa el procedimiento de inicio de sesión para un grupo de trabajo, Access conecta, de forma invisible, a todos los usuarios utilizando la cuenta de usuario **Administrador** predeterminada con una contraseña en blanco. Access utiliza la cuenta de Administrador, en el trasfondo, como cuenta de administrador para el grupo de trabajo, además de actuar como propietario de cualquier base de datos y tablas, consultas, formularios y macros creadas.

Los administradores y propietarios son importantes ya que disponen de permisos que no les pueden ser retirados:

- Los Administradores (miembros del grupo Administradores) siempre pueden obtener permisos sobre los objetos creados en un grupo de trabajo.
- Una cuenta que sea propietaria de una tabla, consulta, formulario, informe o macro siempre puede obtener permisos totales sobre el mismo.
- Una cuenta que sea propietaria de una base de datos siempre podrá abrir la base de datos.

Como la cuenta de usuario de Administrador, es exactamente igual para todas las copias de Microsoft Access, los primeros pasos a seguir para proteger una base de datos son los de definir las cuentas de usuarios de administrador y de propietario (*o utilizar una única cuenta de usuario tanto para la cuenta de administrador como la de propietario*), y después retirar la cuenta de usuario Administrador del grupo Administradores. De lo contrario, cualquiera que disponga de una copia de Microsoft Access podrá conectar con un grupo de trabajo utilizando la cuenta Administrador y disponer de permisos para las tablas, consultas, formularios, informes y macros del grupo de trabajo.

Veamos un ejemplo, para proteger una base de datos titulada **Gestión Clientes**, se podrá crear un **AdminClien** propio, así como cuentas de usuario **PropietarioClien** y después agregar una contraseña a estas cuentas.

Al grupo Administradores se le pueden agregar el número de cuentas de usuario que se deseen, pero solamente una cuenta de usuario podrá ser propietaria de la base de datos (aquella cuenta de usuario que se encuentre activada en el momento de crearse la base de datos, o cuando el título de propiedad se transfiera mediante la creación de una nueva base de datos y se importen todos los objetos de una base de datos en la misma). No obstante, las cuentas de

grupo pueden ser propietarias de tablas, consultas, formularios, informes y macros dentro de una base de datos.

A tener en cuenta

- Las cuentas que se creen para usuarios de la base de datos deberán guardarse en el archivo de información del grupo de trabajo que esos usuarios compartan cuando utilicen la base de datos. En el caso de que se utilice un archivo diferente para crear la base de datos, deberá cambiarse el archivo antes de crear las cuentas.
- Deberá asegurarse de que crea una contraseña única para las cuentas de usuario y de administrador. El usuario que pueda conectarse utilizando la cuenta de administrador siempre podrá obtener permiso total para cualquier tabla, consulta, formulario, informe y macro creados en el grupo de trabajo. El usuario que pueda conectarse utilizando una cuenta de propietario siempre podrá obtener permisos totales para aquéllos objetos que sean propiedad del usuario.

La organización de usuarios por **grupos** facilita la administración segura de una base de datos. Mediante esta estrategia, en lugar de asignar permisos a cada usuario y para cada tabla, consulta, formulario, informe y macro de una base de datos, se podrán asignar permisos a unos pocos grupos y, después, agregar usuarios al grupo apropiado. Cuando los usuarios conectan con Access, adquieren los permisos de cualquiera de los grupos a los cuales pertenezcan. Únicamente las cuentas de usuario podrán conectarse a Access, no es posible conectarse utilizando una cuenta de grupo.

Ejemplo: se podría proteger una base de datos de Pedidos mediante la creación de un grupo Directivos para los directores, un grupo Representantes Comerciales para representantes y un grupo Plantilla para empleados de plantilla. Se podrán asignar los permisos menos restringidos al grupo Directivos, unos permisos más restrictivos al grupo Representantes comerciales y los permisos de mayor restricción al grupo Plantilla. Cuando se crea una cuenta de usuario para un nuevo empleado, se puede agregar esa cuenta al grupo apropiado. El empleado, en consecuencia, dispone de los permisos asociados al grupo.

Una vez creadas las cuentas de usuario y grupo, se podrán visualizar las asociaciones entre los mismos haciendo clic en **Cuentas de usuario y grupo** en el submenú **Seguridad** (menú **Herramientas**), y después haciendo clic en el botón **Imprimir usuarios y grupos**. Microsoft Access imprimirá un informe de las cuentas del grupo de trabajo, mostrando los grupos a los que pertenece cada usuario y los usuarios que pertenecen a cada grupo.

Archivo de información de grupo de trabajo

Es el archivo que Access lee al iniciar la aplicación y que contiene información sobre los usuarios de un grupo de trabajo. Esta información incluye los nombres de las cuentas de usuario, sus contraseñas y los grupos a que pertenecen.

Observaciones sobre las versiones de Access

- En Microsoft Access 95 y versiones anteriores, la información sobre las preferencias de cada usuario (especificada en el cuadro de diálogo Opciones) se guarda en el archivo de información de grupo de trabajo. En Microsoft Access 97 y posterior, la información sobre las preferencias se guarda en el Registro de Windows.
- En la versión 2.0 de Microsoft Access, el nombre predeterminado para el archivo de información de grupo de trabajo es **SYSTEM.MDA**. En ocasiones, se denomina simplemente "grupo de trabajo" o "base de datos del sistema". En Microsoft Access 95 y posterior el nombre predeterminado para este archivo es **SYSTEM.MDW**.