Jose Ignacio González Gómez.
Departamento de Economía Financiera y Contabilidad
Universidad de La Laguna
www.ecofin.ull.es/users/jggomez.

Tema:

SEGURIDAD ACCESS

1º Borrador Revisado: 2006

Indice

1. Aspectos Generales de la Seguridad Basada en Usuarios.

1.1. Introducción.

La seguridad por usuarios de Microsoft Access es muy similar a los mecanismos de seguridad de los sistemas basados en servidor. Mediante el uso de contraseñas y permisos (conjunto de atributos que especifica el tipo de acceso que tiene un usuario a los datos u objetos de una base de datos.),, se puede conceder o limitar el acceso de usuarios o grupos de usuarios a los objetos de una base de datos.

Los permisos se conceden a los grupos y usuarios en la que se establece la forma de trabajar con cada tabla, consulta, formulario, informe, macro de una base de datos.

1.2. Existencia de un fichero de seguridad MDW

Cada vez que los usuarios abren una base de datos, Access tiene que saber quien es el usuario que la abre, por defecto y con el archivo de seguridad preconfigurado SYSTEM.MDW el usuario por defecto es Admin que no tiene clave y tiene asignado todos los privilegios es decir todos los permisos para todos los objetos de la base de datos.

Cuando queremos asegurar una base de datos no queremos por tanto que todo el mundo pueda abrirla con todos los permisos para todos los objetos, por lo que es preciso crear un nuevo fichero de seguridad asociada a esa base de datos y crear usuarios tradicionales con permisos especificos.

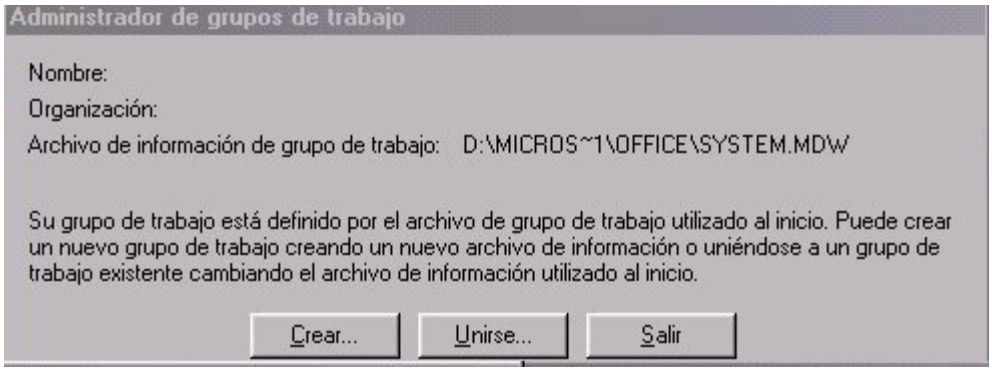
Toda la información sobre la seguridad de las bases de datos Access se guardan en un fichero con extensión MDW o MDA, en los cuales se almacena entre otros datos las configuraciones de los Grupos de Trabajo y en general todas aquellas variables que tienen que ver con la seguridad de la base de datos.

Así podemos utilizar un solo archivo del grupo para todas las bases de datos o podemos crear difentes grupos de trabajo para disitintas bases de datos, en este último caso implica que deberemos distribuir este fichero de seguridad (que contiene los grupos de trabajo y permisos) con la base de datos asociada a este fichero de seguridad.

De forma predeterminada el fichero del grupo de trabajo con que se abre por defecto nuestras bases de datos es el denominado SYSTEM.MDW.

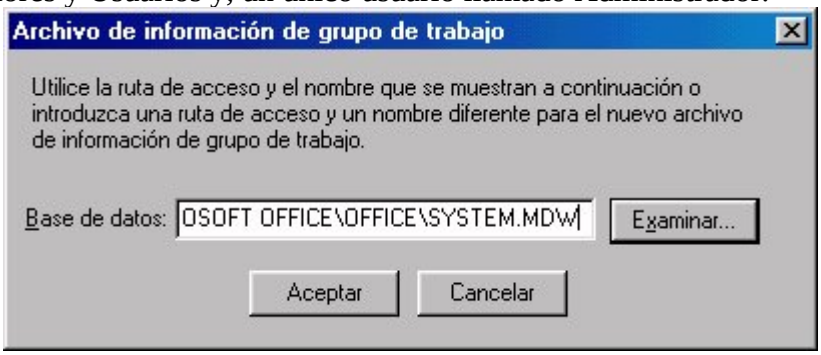
Para acceder a estos ficheros se puede utilizar el ejecutable WRKGADM.EXE que suele encontrarse en el directorio de Access o en el

directorio \Windows\System.



El nombre que suele aparecer para el ejecutable es, Administrador para trabajo en grupo.

Access trae por defecto un fichero el SYSTEM.MDW (SYSTEM.MDA en Access 2), normalmente en el mismo directorio, el cual contiene dos Grupos de usuarios: Administradores y Usuarios y, un único usuario llamado Administrador.



1.3. Objetivos del fichero de seguridad

Mediante las herramientas de Access, vamos a procurarnos una seguridad bastante buena en nuestras BD.

1. Disponer de una Base de Datos que, solo la persona que disponga de un archivo xxxxxxxx.MDW determinado que además conozca un código de usuario concreto y su contraseña asociada, sea capaz de entrar en ella.
2. Esta persona, que será la propietaria de la base de datos, podrá crear grupos de usuario y usuarios a los que podrá dar autorizaciones de uso concretas.
3. Nadie podrá llevarse la base de datos SEGURA a otro sistema Access y acceder a ella, ni como administrador, ni como ningún otro usuario, excepto que se haya llevado también nuestro xxxxxxxx.MDW y sepa además, nuestro código de usuario y nuestra contraseña.

Por tanto, el mejor método para ayudar a proteger una base de datos se denomina seguridad por usuarios. Las dos razones principales para utilizar seguridad por usuarios son:

- Impedir que los usuarios cambien o inutilicen inadvertidamente una aplicación cambiando tablas, consultas, formularios, informes y macros de los que depende la aplicación.
- Ayudar a proteger los datos importantes de la base de datos.

De hecho, la seguridad en Microsoft Access siempre está activada. Hasta el momento en que se activa el procedimiento de inicio de sesión para un grupo de trabajo, Microsoft Access conecta a todos los usuarios, de forma imperceptible, con la cuenta de usuario Administrador (cuenta Administrador: cuenta de usuario predeterminada. Cuando se instala Access, el programa de instalación incluye la cuenta de usuario Administrador en el archivo de información de grupos de trabajo que crea.) Predeterminada y con una contraseña en blanco.

Por tanto uno de los principales pasos será establecer esa seguridad con nombres de usuarios y contraseñas. Es decir, 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.

1.4. Contenido de un fichero de seguridad MDW.

1.4.1. Definición de Grupos de Trabajo Administradores y Grupo de Trabajo Usuarios.

Un grupo de trabajo es una colección de usuarios (grupos de usuarios) y permisos para objetos.

Un grupo de trabajo de Microsoft Access es un grupo de usuarios en un entorno multiusuario que comparten datos.

Si está definida la seguridad por usuarios, los miembros de un grupo de trabajo quedan registrados en las cuentas de usuario y de grupo que se almacenan en un archivo de información del grupo de trabajo de Microsoft Access.

En términos de seguridad una cuenta de grupo de trabajo es una colección de cuentas de usuario de un grupo de trabajo, identificado por un nombre de grupo y un Id. personal (PID). Los permisos asignados a un grupo se aplican a todos los usuarios del grupo.). Al incluir un usuario

Las cuentas de seguridad definen los usuarios y grupos de usuarios que tienen acceso a los objetos de la base de datos. Esta información, que se conoce con el nombre de grupo de trabajo, se almacena en un archivo de información del grupo de trabajo.

Un archivo de información del grupo de trabajo de Microsoft 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 pueden utilizar el motor de base de datos Microsoft Jet, como Microsoft Visual Basic para aplicaciones (VBA) y Microsoft Excel.
Administradores	La cuenta de grupo del administrador. Esta cuenta es única para cada archivo de información de grupo de trabajo. De forma predeterminada, el usuario Administrador pertenece al grupo

Administradores. Como mínimo, deberá haber en todo momento un usuario en el grupo Administradores.

Usuarios

La cuenta de grupo que comprende todas las cuentas de usuario. Cuando un miembro del grupo Administradores crea una cuenta de usuario, Microsoft 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 totales para 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 dicho usuario.

1.4.2. Grupos de trabajos predeterminados: Administradores y Usuarios

Por tanto a los usuarios se les obliga a identificarse y escribir una contraseña cuando inician Microsoft Access.

Microsoft Access ofrece dos grupos predeterminados de trabajo:

- Grupo de Trabajo Administradores.
- Grupo de Trabajo Usuarios.

Evidentemente se pueden crear grupos de trabajo adicionales con la configuración de permisos deseada.

Al grupo Administradores se le puede asignar el número de cuentas de usuario que se desee, pero sólo una cuenta de usuario podrá ser propietaria de la base datos, es decir, la cuenta de usuario activa en el momento de crear la base de datos o en el momento de transferir la propiedad mediante la creación de una nueva base de datos y la importación a ésta de todos los objetos de la base de datos anterior. No obstante, las cuentas de grupo pueden ser propietarias de tablas, consultas, formularios, informes y macros dentro de una base de datos.

2. Sobre el fichero de seguridad por defecto de Access. SYSTEM.MDW.

2.1. Como inicia una sesión Access y carga su fichero de seguridad por defecto.

Por defecto cuando se abre una base de datos se carga un sistema de seguridad totalmente abierto que se denomina SYSTEM.MDW para comprobarlo, carguemos cualquier base de datos o simplemente abrimos la aplicación MS Access y vamos a la opción Herramientas-Seguridad-Administración de Grupos de Trabajo.

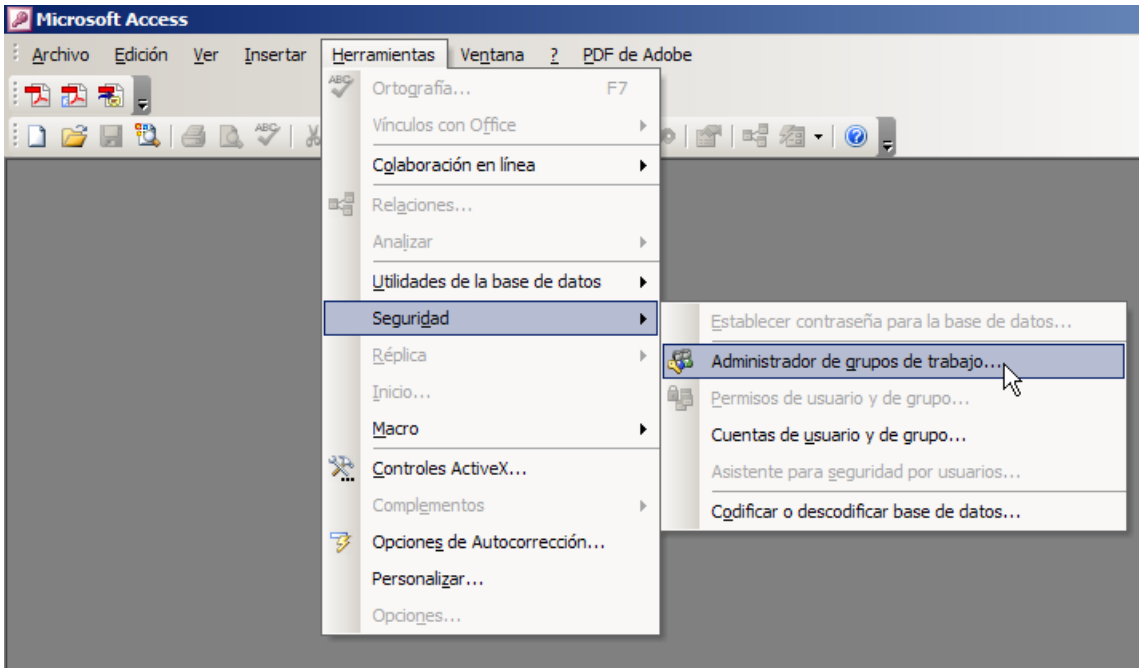


Ilustración 1

De esta forma se abre el siguiente cuadro de dialogo (Ilustración 2) que nos informa a que fichero o grupo de seguridad nos hemos conectado, si queremos iniciar la sesión de Access con otro fichero de seguridad o si queremos crear y configurar uno propio.

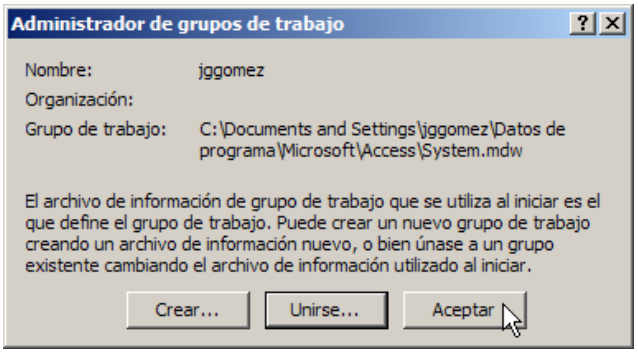


Ilustración 2

Como hemos dicho los ficheros de seguridad tienen la extensión "**mdw**" y por defecto el fichero que se carga cada vez que se abre el Access es el "SYSTEM.MDW" que se encuentra normalmente en la siguiente ruta:

C:\Documents and Settings\usuario xxxx\Datos de programa\Microsoft\Access

Esto significa que por defecto cada vez que abrimos Access este se inicia con una sesión de seguridad predefinida por los valores contenidos en el fichero, es decir por los distintos Grupos de Usuarios (básicamente Grupo de Administradores y Grupo de Usuarios) así como los permisos asociados a cada Grupo de Usuarios y por los usuarios concretos que deben pertenecer algún Grupo definidos anteriormente.

2.2. Preservar el fichero de seguridad por defecto, SYSTEM.MDW

Con el fin de evitar cometer errores de forma irreparable, consideramos necesario resguardar y hacer una copia del fichero de seguridad que por defecto con las que se abren todas nuestras bases de datos. Para ello simplemente acudimos a la ruta donde el mismo se encuentra, recordemos C:\Documents and Settings\usuario xxxx\Datos de programa\Microsoft\Access y lo copiamos en otra carpeta a buen resguardo para que en caso necesario podamos remplazarlo.

2.3. Contenido del fichero de seguridad de Access.

2.3.1. Inspeccionar el contenido del fichero de seguridad.

Una vez que hemos abierto la aplicación Acces y cargada cualquier base de datos que hemos elaborado podemos observar como por defecto se ha cargado también el fichero de seguridad “SYSTEM.MDW”.

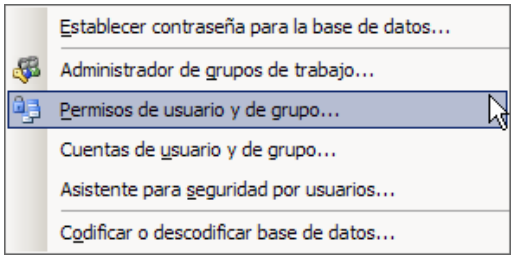


Ilustración 3

Las propiedades y configuración de este fichero se pueden analizar a través de dos opciones a las que se accede de la selección Herramientas y Seguridad que nos llevara a centrar nuestra atención en las dos opciones siguientes:

- Permisos de usuarios y grupo
- Cuenta de usuario y de grupo.

Señalar que la opción Administrador de grupos de trabajo simplemente nos sirve para conocer a que fichero de seguridad (mdw) estamos conectados, a crear un nuevo fichero o a unirnos a un nuevo.

Por otro lado el asistente para seguridad por usuarios nos llevará a la creación de un nuevo fichero de seguridad como posteriormente tendremos oportunidad de analizar.

2.3.2. Los permisos de usuarios y de grupo por defecto en el fichero de seguridad SYSTEM.MDW.

Retomando la Ilustración 3, en esta opción podremos analizar y modificar los permisos de los usuarios y de grupo que se encuentran configurados en el fichero de seguridad con el que hemos abierto la sesión de Access.

Los permisos, son básicamente los privilegios específicos de acceso a la información y a los recursos de la base de datos.

En este sentido todos los permisos se encuentran organizados en dos grandes grupos, permisos de grupos y permisos de usuarios.

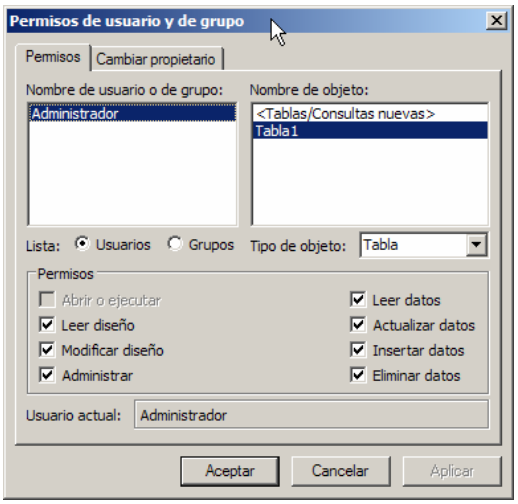


Ilustración 4

Las cuentas de usuarios son cuentas que identifican por un nombre de usuario y un Id. personal (PID) a una persona concreta, asignándole los permisos correspondientes para tener acceso a la información y a los objetos de base de datos en un grupo de trabajo de Access.

Una cuenta de grupo es una colección de usuarios identificado por un nombre de grupo y un Id. personal (PID) que contienen un conjunto de permisos asignados al grupo para controlar y administrar los permisos y el acceso de este grupo a los objetos de la base de datos.

Para entenderlo mejor supongamos una gran base de datos de carácter empresarial que guarda información económica, financiera y comercial de la empresa. Debemos limitar

el acceso a la información, axial por tanto crearemos grandes grupos de usuarios en base al departamento al que cada uno pertenece, es decir crearemos los siguientes Grupos de Trabajo:

- Grupo de Trabajo “Comerciales”
- Grupo de Trabajo “ Administrativos”
- Grupo de Trabajo “ Gerencia”

Esto nos permitirá configurar perfiles de usuarios con acceso a determinada tipo de información de interés para cada uno de estos Grupos de Trabajo. Pero dentro de cada Grupo de Trabajo abra usuarios con preferencias o acceso a información diferentes, así por ejemplo dentro de los Comerciales tendremos a los Vendedores, Jefes de Equipo de Ventas, Directores Comerciales a los cuales podremos personalizar el acceso a la información a través de sus permisos concretos.

Todo ello se realiza, como hemos comentado, a través de la opción del programa Herramientas, Seguridad, Permisos de Usuarios y de Grupos.

Es aconsejable seguir el siguiente orden en el proceso del establecimiento de los permisos:

1. Crear los grupos de trabajos más generales.
2. Definir los permisos de estos grupos trabajos
3. Crear los usuarios y asignarlos a los grupos de trabajo
4. Personalizar los permisos de cada uno de los usuario de cada grupo de trabajo.

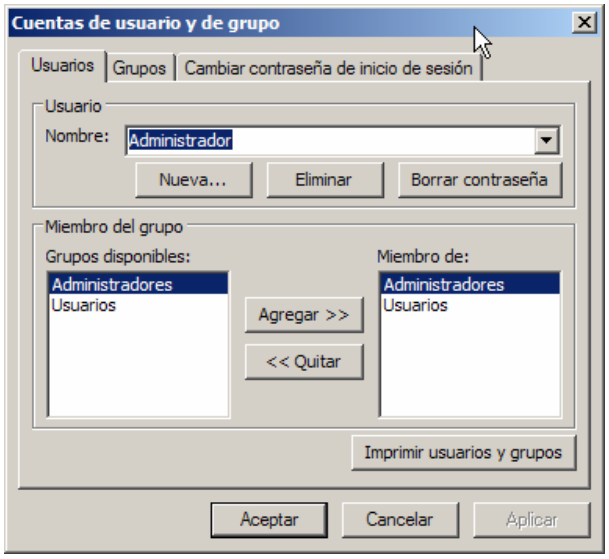


Ilustración 5

Si queremos ver los Grupos de Trabajo que por defecto tenemos creado en el fichero base SYSTEM. MDW tendremos que acudir a la opción Herramientas-Sistemas-Cuentas de Usuarios y Grupo (ver Ilustración 3) que nos da acceso a una nueva ventana en las que se nos informa de cada uno de los usuarios y el grupo al que pertenece así como la posibilidad de poder definir una contraseña de inicio para cada usuario.

3. Proteger una base de datos con un fichero de seguridad personalizado MDW.

3.1. Necesidad de crear un nuevo fichero de seguridad

Es altamente aconsejable crear un nuevo archivo de seguridad asociada a la base de datos que queremos resguardar y no machacar la que por defecto se conectan todas las bases de datos del sistema que es la SYSTEM.MDW. De esta forma asociaremos exclusivamente el fichero de seguridad nuevo que vamos a crear, xxxxxxxx.MDW

exclusivamente a la base de datos que queremos proteger y no a todas las bases de datos del sistemas.

3.2. Uso del Asistente.

3.2.1. Crear un fichero de seguridad propio asociado a la base de datos.

En primer lugar debemos abrir la base de datos que deseamos configurar para su sistema de seguridad, para ello una vez abierta la misma vamos a la opción Herramientas-Seguridad- Asistente para Seguridad por Usuarios.

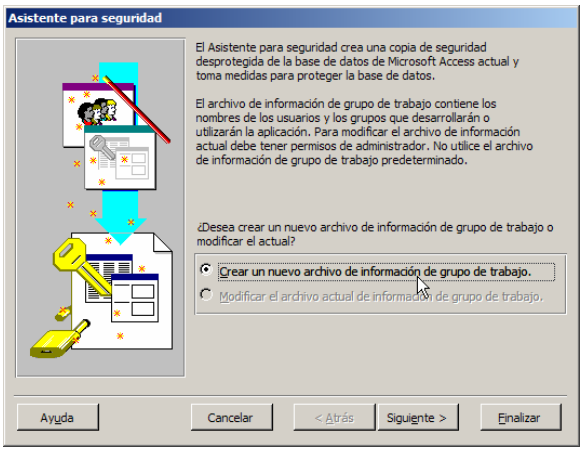


Ilustración 6

Por tanto nuestro primer paso es crear un nuevo fichero para trabajo en grupo, es decir un nuevo MDW el cual aconsejamos ubicarlo en el mismo directorio en el que se encuentra la base de datos que se pretende asegurar. Por defecto, al crearlo, Access queda conectado a dicho grupo de seguridad. Se puede comprobar saliendo y volviendo a entrar.

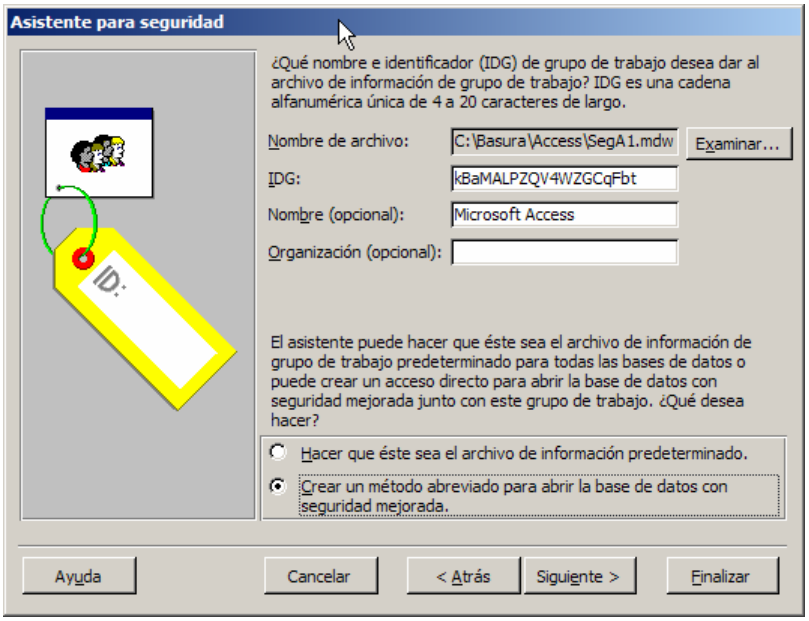


Ilustración 7

Por tanto es importante seleccionar la opción 2 y no la de establecer que este archivo de información sea el predeterminado en cuanto que afectaría a todas las bases de datos de nuestro sistema.

En el botón examinar seleccionaremos el directorio y el nombre del nuevo fichero de seguridad que queremos generar y donde se debe guardar este, aconsejamos que se guarde en el mismo lugar donde tenemos almacenada la base de datos, es decir en el mismo directorio, en nuestro caso hemos seleccionado como nombre SegA2.mdw

3.2.2. Selección de elementos objeto de protección

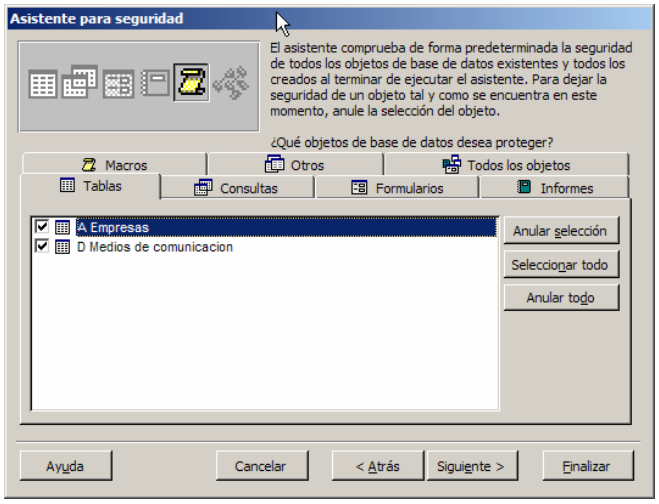


Ilustración 8

Posteriormente al paso anterior comenzaremos por definir cuales son los elementos que deseamos proteger, tablas, consultas, formularios, informes y macros.

En este punto podemos dejar las opciones por defecto como están, es decir proteger todos los objetos de las base datos y en tal caso al finalizar el asistente podremos cambiar los parámetros de protección, como veremos posteriormente

3.2.3. Creación de Grupos con el Asistente.

Por defecto con el asistente se generan automáticamente dos grupos de trabajo:

- Grupo de Trabajo Administradores
- Grupo de Trabajo Usuarios

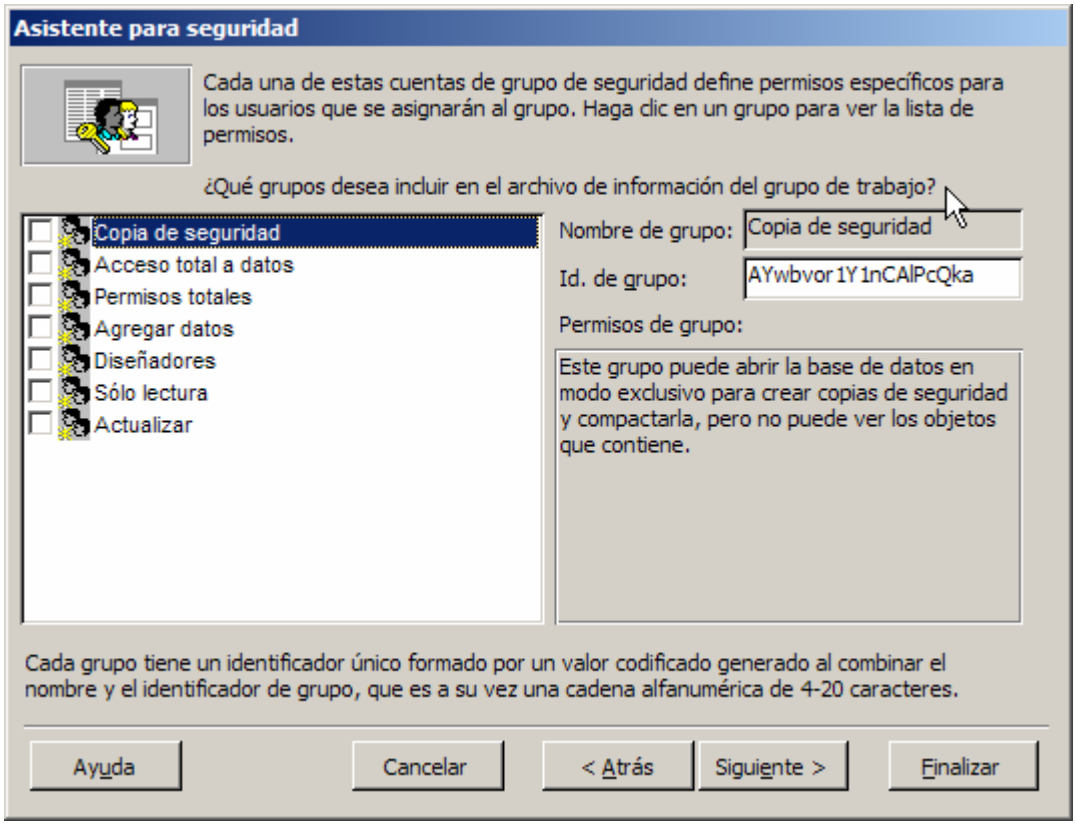


Ilustración 9

No obstante el asistente nos posibilita crear nuevos grupos de trabajo como los que se muestran en la Ilustración 9 con sus permisos concretos, en principio es suficiente con los dos que por defecto se generan, los de Administradores y Usuarios.

Recordar que posteriormente podremos crear nuevos grupos y establecer sus perfiles a través de la opción mostrada en la Ilustración 3.

3.2.4. Concesión de permisos al Grupo Usuarios

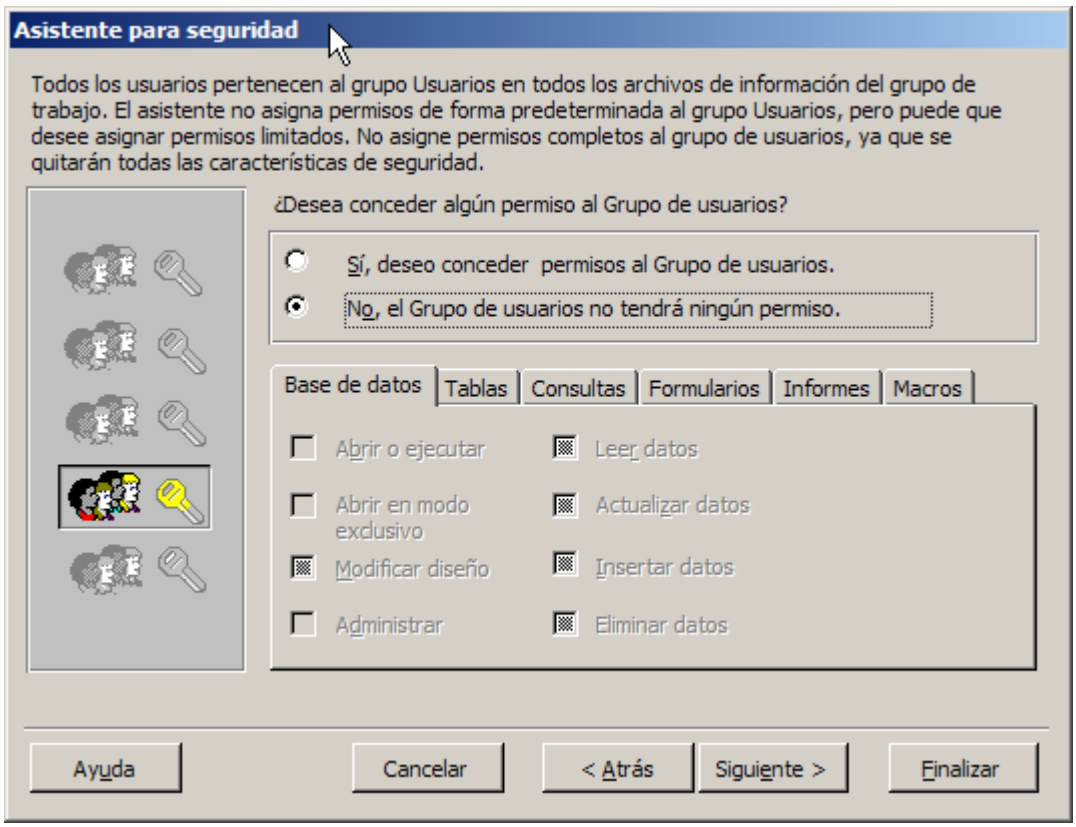


Ilustración 10

El Grupo de Usuarios podrá tener definidos permisos concretos, en este sentido seleccionaremos la primera opción pero tal como nos aconseja es mejor no definir ningún permiso al grupo de usuarios para tener perfectamente limitado el acceso, aunque evidentemente podremos modificarlo posteriormente.

3.2.5. Alta del Nuevo usuario Administrador con Clave y de Usuario Gral.

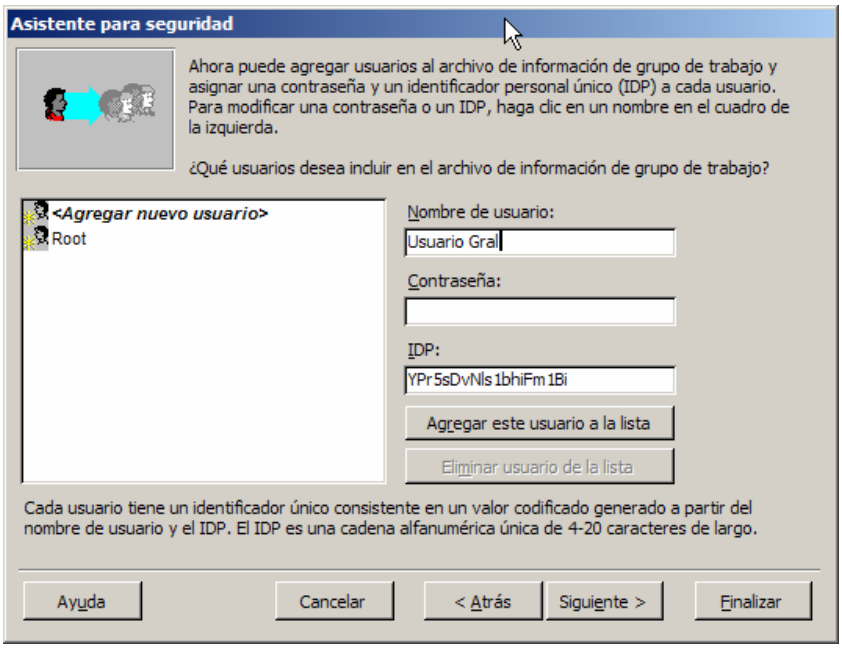


Ilustración 11

El Asistente nos llevará a continuación a una nueva pestaña en la que ***es importante*** dar de alta a un nuevo Administrador con nombre distinto al que esta por defecto y con una clave, en nuestro caso la hemos denominado Root con la clave asignada como 1234.

Se podrán dar aquí de alta a otros usuarios generales así como eliminar otros usuarios.

Por tanto hemos creado dos cuentas tal y como se muestra en la Ilustración 11 un futuro Administrador con Clave que llamaremos Root (con clave 1234) y Usuario Gral (sin clave).

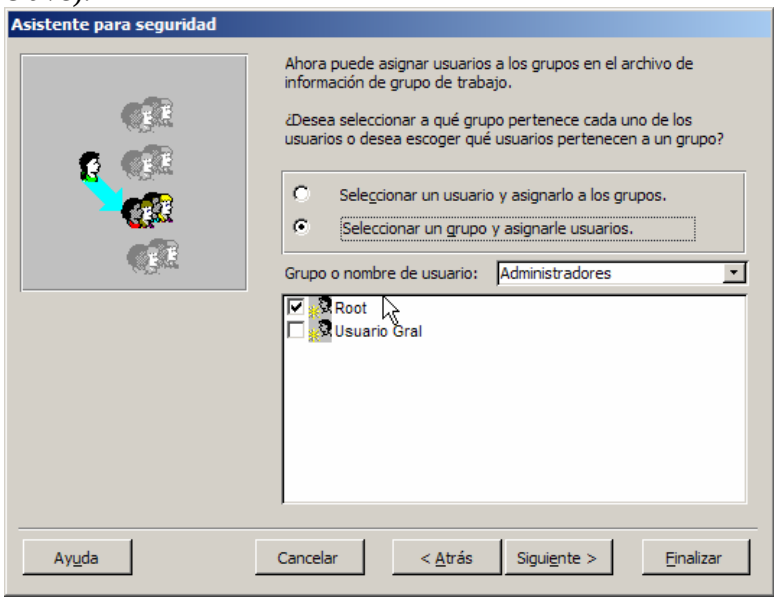
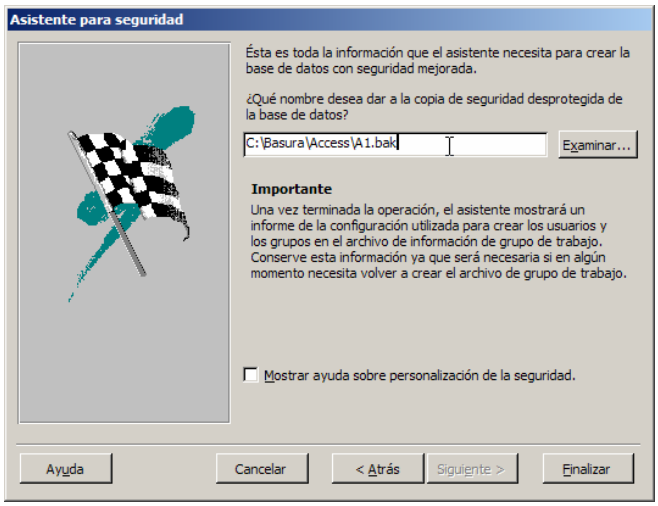


Ilustración 12

Solo nos falta a continuación asignar los usuarios a los grupos de trabajo, para ello accedemos a la siguiente pantalla (Ilustración 12), donde solo pondremos en el Grupo de Trabajo Administradores al Root que tiene clave asignada y al resto de miembros no lo asignaremos al Grupo de Usuarios. Si hubiera algún otro usuario en el Grupo de Administradores lo borraríamos de ahí.

3.2.6. Últimos pasos del asistente. Copia de seguridad de la base de datos e impresión de fichero de seguridad.



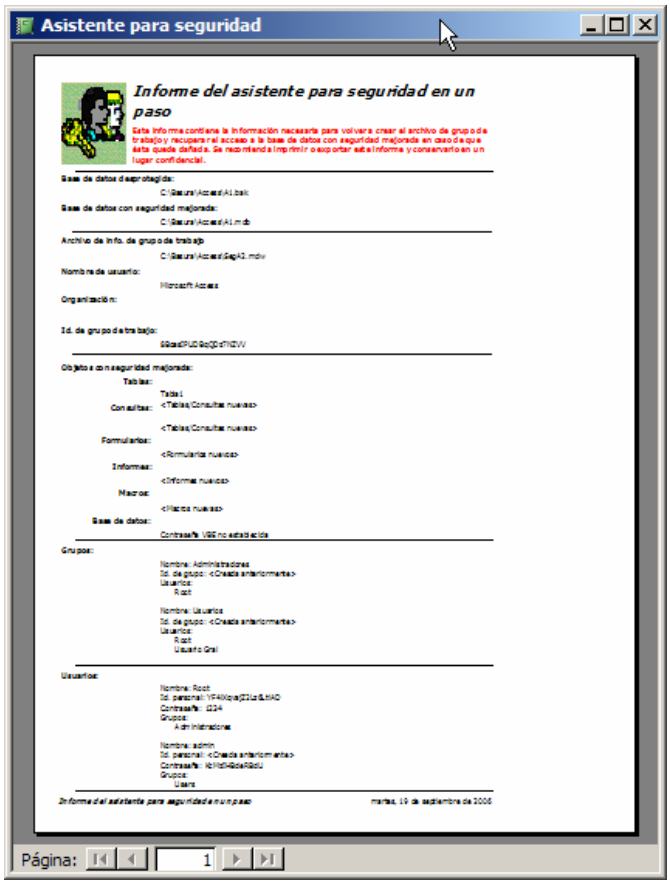


Ilustración 13

Finalmente se nos genera una copia de seguridad de la base de datos en el mismo directorio que por defecto tenemos almacenada nuestra base de datos de trabajo, así como al pulsar sobre el botón seguir se genera un informe automáticamente referente a los parámetros básicos del fichero de seguridad generado que debemos guardar en un lugar seguro.

3.3. El acceso directo generado.

Una vez terminado el asistente, ***debemos fijarnos en un detalle muy importante***, se ha generado un icono de acceso directo en nuestro escritorio con el nombre de la base de datos y en la que dentro de sus propiedades aparece una instrucción en el campo destino, ver Ilustración 14.

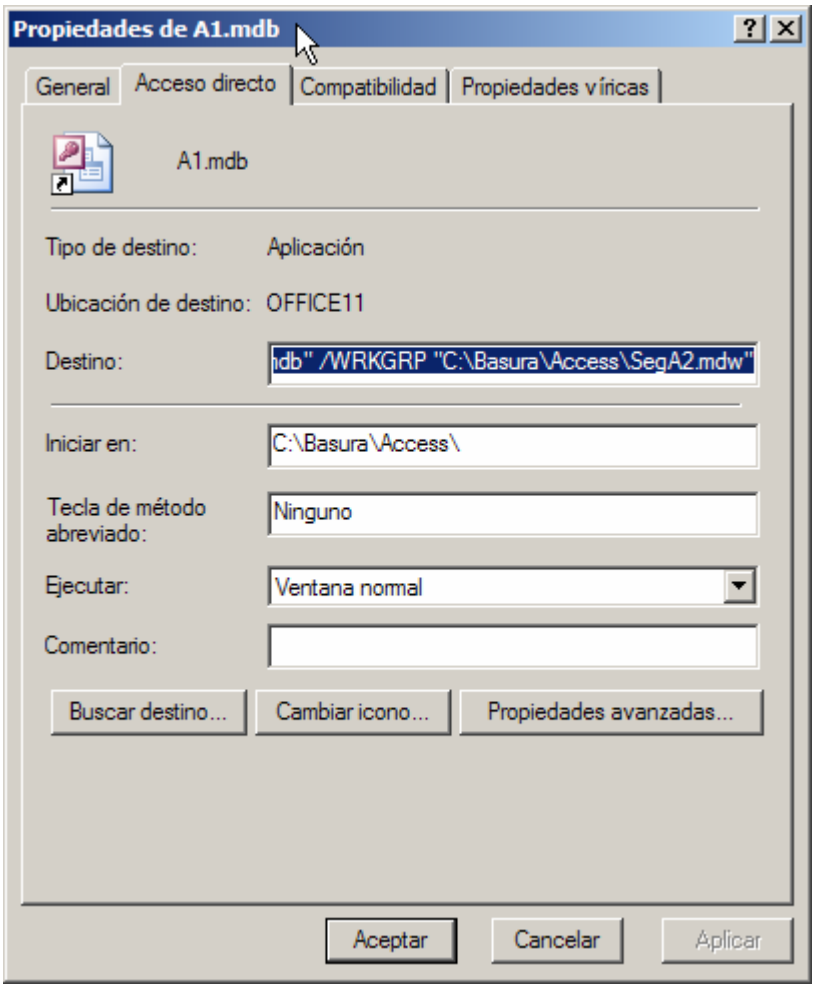


Ilustración 14

"C:\Archivos de programa\Microsoft Office\OFFICE11\MSACCESS.EXE" "C:\Basura\Access\A1.mdb" /WRKGRP "C:\Basura\Access\SegA2.mdw"

Esto significa, que cuando ejecute el acceso directo abra en primer lugar el Access que se encuentra en la ruta señalada (C:\Archivos de programa \Microsoft Office\OFFICE11\ MSACCESS.EXE) y posteriormente cargue la base de datos del lugar establecido (C:\Basura\Access\A1.mdb) que lleva asociada un fichero de seguridad a la misma que también será cargado y que se encuentra en la ruta especificada (C:\Basura\Access\SegA2.mdw).

Por tanto si cambiamos de directorio nuestra base de datos y nuestro fichero de seguridad tendremos que modificar el fichero de acceso directo generado.

3.4. Cargar la base de datos protegida y distribución de la aplicación. Los tres ficheros mágicos.

Por tanto siempre que queramos abrir esta base de datos A1.mdb que se encuentra protegida a nivel de usuario tendremos que hacerlo a través del fichero de acceso directo que se ha generado.

Esto implica que si vamos a distribuir esta aplicación es recomendable ubicar los tres ficheros básicos: la base datos, el fichero de seguridad y el acceso directo en un mismo directorio y fijarnos que la propiedad del acceso directo no ha cambio o ajustarla a los nuevos parámetros o rutas.

3.5. Reestablecer como fichero de configuración predeterminado de Access el SYSTEM.mdw.

Puede darse el caso, por cualquier circunstancia que nuestro fichero de seguridad que por defecto abre el Acces no sea el genérico sino el privado o el que hemos adaptado para una base de datos concreta, hemos por tanto modificar esta opción y decirle a la aplicación que nos abra el fichero deseado.

Para ello abrimos la aplicación Microsoft Access sin cargar ninguna base de datos y seleccionamos Herramientas-Seguridad-Adminsitración de Grupos de Trabajo, tal y como se muestra en la Ilustración 3, lo que nos lleva a un nuevo cuadro de dialogo como el presentado en la siguiente Ilustración

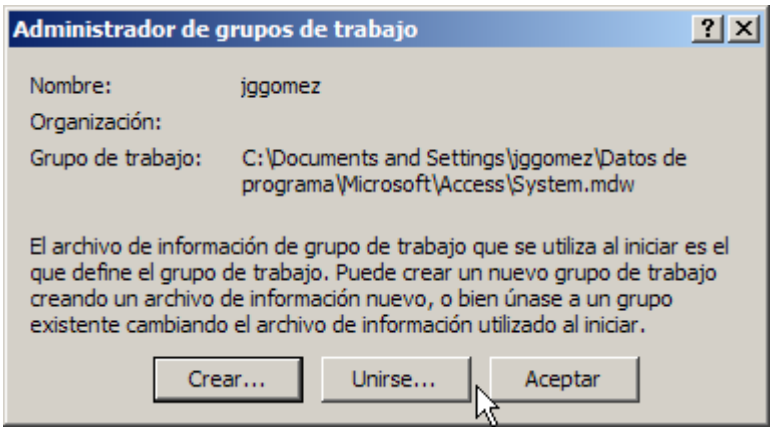


Ilustración 15

En esta nos indica el fichero de seguridad que se ha cargado así como nos da la posibilidad de generar uno nuevo o cargar uno previamente existente.

Recordemos una vez más que Access guarda por defecto los ficheros de seguridad en el directorio:

C:\Documents and Settings**usuario xxxx**\Datos de programa\Microsoft\Access, donde **usuario xxxx** es la carpeta por defecto del usuario que ha iniciado la sesión del sistema operativo. En este sitio encontraremos las distintas versiones de la modificación del fichero que por defecto usa Access como seguridad para las bases de datos que abrimos.

Si por cualquier circunstancias hemos machacado este fichero nos encontraremos con la desagradable situación que nuestras bases de datos no se podrán abrir, para lo cual una solución seria acudir a otro ordenador, copiar su fichero SYSTEM.mdw que no haya sido modificado y remplazarlo por el nuestro en la ruta por defecto indicada.

4. Configuración y adaptación del fichero de seguridad personalizado.

4.1. Introducción.

Una vez creado el fichero de seguridad podremos crear nuevos grupos de trabajo o configurar los mismos, dar de alta a usuarios y asignarlos a los grupos de trabajo, establecer contraseñas para los usuarios, diseñar los permisos de acceso, etc.

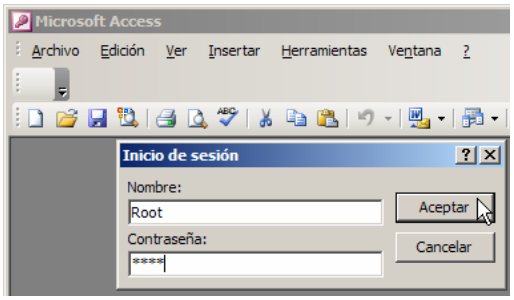


Ilustración 16

Para ello comenzaremos accediendo a nuestra base de datos protegida a través del acceso directo generado que nos abrirá el programa Microsoft Acces y cargara la base de datos y el fichero de seguridad asociada a la misma. Como podemos observar nos pide primero que nos identifiquemos para acceder a la misma.

Para ello debemos en primer lugar cargar el fichero de seguridad sobre el que queremos establecer las configuraciones y para ello procederemos en primer lugar abriendo el Acc

4.2. Como crear y eliminar usuarios y asignarlos a un grupo. Creando una contraseña a los usuarios.

Una vez dentro de la base de datos con seguridad de usuarios accedemos a la opción del programa Herramientas-Seguridad-Cuentas de Usuarios y Grupos.

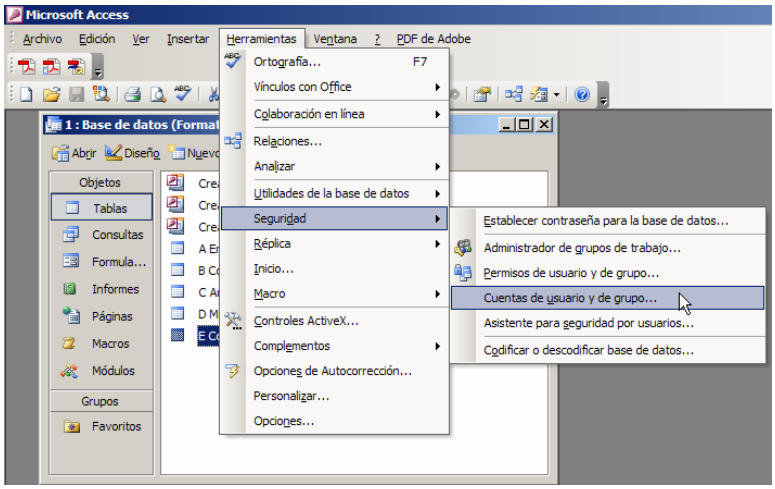


Ilustración 17

De esta forma accedemos a los parámetros de nuestro fichero de seguridad donde se guarda toda la configuración de grupos, usuarios y permisos. Así la pestaña Usuarios se compone de dos apartados:

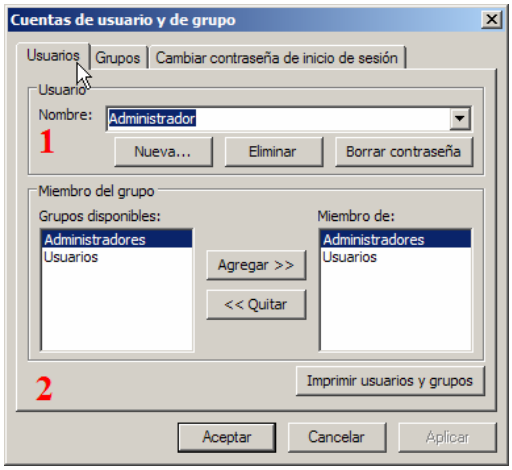


Ilustración 18

1. La primera se utiliza para mantener los nombres y contraseñas de los usuarios.
2. La segunda se utiliza para asignar usuarios a grupos.

Así para crear un usuario nuevo pulsamos sobre el botón nuevo de la Ilustración 18 con lo que nos aparecerá un nuevo cuadro de dialogo (Ilustración 19).

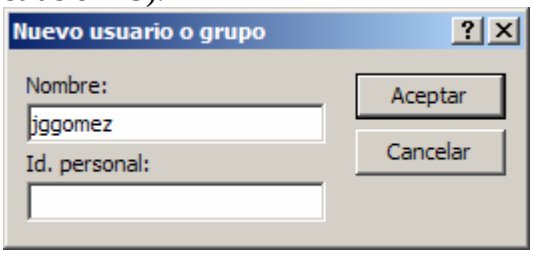


Ilustración 19

En este último cuadro de dialogo tendremos que asignar el nombre del usuario y un ID de control que tendrá que ser como mínimo de cuatro caracteres y máximo 20, pulsando sobre el botón aceptar el usuario quedará creado.

Recomendamos dar de alta a todos los usuarios que deseemos desde esta opción del programa y asignarlos al grupo de trabajo deseado (Administradores o Usuarios).

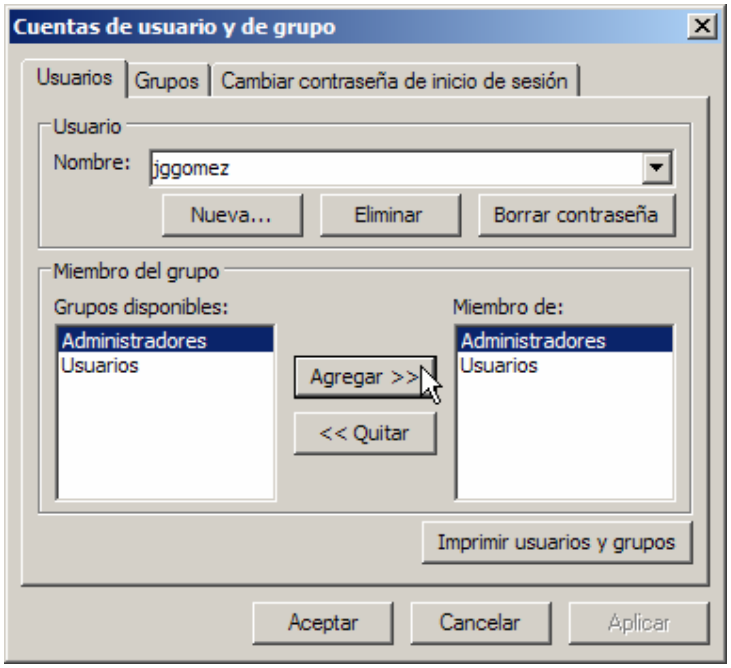


Ilustración 20

Una vez creado el usuario, debemos asignarlo a un grupo, en nuestro caso asignaremos el usuario jggomez al grupo de Administradores, para ello y tal como se muestra en la Ilustración 20, seleccionado el usuario deseado, en el área Miembro del Grupo, seleccionamos Administradores y le damos al botón agregar, de esta forma el usuario jggomez con su contraseña pertenecerá al grupo Administradores y Usuarios heredando todos los privielgios asignados a los mismos.

Hay que tener en cuenta y que si hemos accedido a la base de datos como Administrador y queremos cambiar la contraseña de un usuario, es necesario salir de la aplicación y entrar con el nombre del usuario que queremos cambiar, es él y solo él (ese usuario) el que la podrá cambiar o modificar su contraseña.

Por defecto Access en su fichero de seguridad genera un usuario por defecto que es " Administrador" y que pertenece al grupo de trabajo de administradores y usuarios, por lo tanto lo primero que tenemos que hacer recordemos es:

- Crear un nuevo usuario (por ejemplo Root) que pertenezca a estos dos grupos de trabajo administradores y usuarios
- Desvincular al Administrador del grupo de trabajo Administradores, para que no tenga permisos de variar la configuración de seguridad. Debemos tener presente que el Administrador este solo asignado al Grupo de Usuarios, pero nunca al de Administradores y si lo esta debería estarlo con clave.
- Salir de la base de datos y volver a entrar a través del acceso directo y como nuevo administrador (root) y establecer una contraseña para el mismo.

De esta forma la administración de la seguridad de la base de datos queda garantizada pero teniendo en cuenta que el grupo de trabajo usuarios tiene que tener los permisos limitados, para ello es necesario revisar la configuración de permisos de cada una de los grupos de trabajo.

Por tanto a medida que vayamos creando nuevos usuarios, los vamos uniendo a los distintos grupos creados según nuestra planificación de seguridad y esto significa que los mismos heredaran los permisos de seguridad establecidos para el grupo de usuarios en el que se encuentran inmersos.

4.3. Sobre la asignación de permisos.

Como podemos ver Access genera por defecto dos grupos genéricos Administradores que es el que tiene todos los permisos y el de usuarios.

4.4. Eliminar el Usuario por Defecto Admin y crear un nuevo administrador con clave.

Por defecto el fichero generado de seguridad contiene un usuario Admin sin clave asignada y que forma parte del grupo Administradores, esto supone por tanto que todo usuario que abra la base de datos, se conectara por defecto como Admin sin clave lo que implica que tendrá todos los permisos concedidos, es necesario por tanto cambiar este usuario para garantizar la seguridad de la base de datos., creando un nuevo usuario con clave, de forma que al abrir la base de datos nos pida el nombre y la clave del nuevo usuario o administrador de la base de datos que tiene control total sobre la misma.

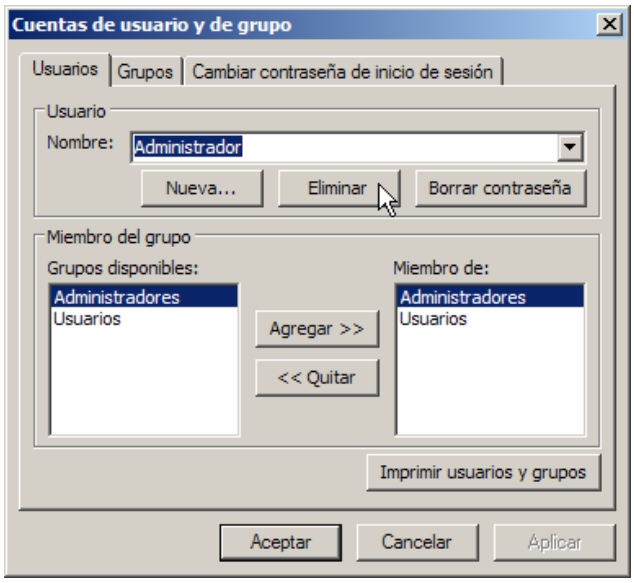


Ilustración 21

Es decir, para asegurar totalmente la base de datos es necesario eliminar todos los permisos del usuario Admin.

Pero para ello es necesario previamente el haber creado otro usuario con clave y perteneciente al grupo de Administradores. Es decir el Grupo de Administradores no puede estar vació debe existir como mínimo un usuario en ese grupo.

Por tanto, suponiendo que ya hemos creado el usuario nuevo Administrador

Para ello, accedemos a la Ilustración 18 y seleccionamos el usuario que deseamos eliminar, en nuestro caso Administrador.

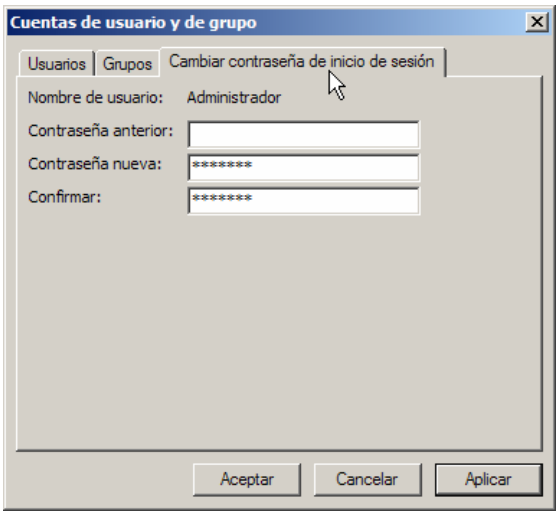
- Intentó eliminar la única cuenta de usuario del grupo Administradores. El grupo Administradores debe tener al menos una cuenta de usuario. Si desea eliminar esta cuenta, cree una nueva cuenta y agréguela al grupo Administradores, o agregue una ya existente al grupo Administradores y luego elimínela.

4.5. Creación o modificación de la Contraseña de Usuario.

Para asignar o establecer una contraseña de usuario debemos acceder a la opción del programa Herramientas-Seguridad-Cuentas de Usuarios y Grupos.

Posteriormente seleccionamos la pestaña cuentas de usuarios y grupos y si el usuario que se ha conectado tiene una contraseña debemos escribirla en el campo anterior, en caso contrario establecemos la misma, confirmándolo en el campo siguiente.

En nuestro caso estamos cambiando la contraseña al Administrador que por defecto no tenia ninguna asignada previamente.



.

5. Bibliografía

http://www.hispavila.com/3ds/office/seguridadaccess.html