

Utilización de Lenguajes de Cuarta Generación (4GL) para la elaboración de pantallas en las Bases de Datos

Manuel León Vega

Universidad de Costa Rica, Escuela de Ciencias de la Computación e Informática
San José, Costa Rica
mlvcr3@gmail.com

and

José A. Romero González

Universidad de Costa Rica, Escuela de Ciencias de la Computación e Informática
San José, Costa Rica
andresromg@gmail.com

Abstract

The data bases are containers of information of fourth generation where the data usually stay centralized assuring integrity the information in contrast to the rudimentary methods used years back. The systems database administrators are in charge to manage the data bases and offer security mechanisms to protect to such as much of errors committed by users or are malicious or not and of faults in the atmosphere. By means of guided tools the generation of screens, information and reports is very simple, Access is an example of a simple tool that if is learned to use of correct way this with the purpose of making agile the production processes could generate friendly data bases.

Keywords: Data, Information, Security, Generator, IMEC

Resumen

Las bases de datos son repositorios de información de cuarta generación donde los datos se mantienen usualmente centralizados asegurando la integridad de la información en contraposición a los métodos rudimentarios utilizados unos años atrás. Los sistemas administradores de bases de datos se encargan de administrar las bases de datos y ofrecen mecanismos de seguridad para proteger a los mismos tanto de errores cometidos por usuarios ya sean malintencionados o no y de fallas en el ambiente. Por medio de herramientas guiadas la generación de pantallas, informes y reportes resulta muy sencillo, Access es un ejemplo de una herramienta simple que si se aprende a utilizar de manera correcta podría generar bases de datos amigables esto con el fin de agilizar los procesos de producción.

Palabras clave: Datos, Información, Seguridad, Generador, IMEC

1 Bases de Datos

Debido al volumen de información que se manipula en la vida cotidiana y la necesidad de persistencia de la misma, se han creado una serie de herramientas, que bajo las demandas presentadas y desarrollo tecnológico actual, permiten no solo almacenar información textual sino además datos multimedia, por medio de las bases de datos.

Dos décadas atrás, la manipulación de la información se realizaba de manera rudimentaria por medio de archivos de texto y expedientes, lo cual provocaba duplicidad de la información, desvirtualización de la información y pérdida de la misma, la razón principal era por la falta de descentralización y seguridad de los datos. Ahora se tiende a restringir el acceso a los datos y a tratar de mantener a los mismos en un solo lugar, esto con el fin de que se trate de mantener la integridad de los mismos. Para comprender mejor lo anterior es conveniente dar una definición formal de lo que es una base de datos.

Una base de datos es una colección de datos relacionados. Por datos, queremos decir hechos conocidos que pueden registrarse y que tienen significado implícito [1].

Dicho concepto resulta un tanto ambiguo, ya que la especificación “implícito” está condicionado a ciertas restricciones, los datos deben estar sujetos a un universo, es decir, estos deben de estar relacionados los uno con los otros, es producto de un interesado en la recopilación y conservación de estos datos, dicha información en conjunto tiene un significado válido al universo sujeto. Además es de considerar que los elementos presentes en el contenedor tienen un mantenimiento que implica inserción, modificación, eliminación y consulta (IMEC) de los mismos.

A parte de ello, la necesidad de que el proceso de creación de aplicaciones se realice de manera rápida, para conseguir esto, se deben de simplificar ciertas etapas en el desarrollo de sistemas. En la actualidad existen herramientas que permiten crear informes, reportes, consultas e incluso pantallas de manera simple y guiada.

2 Interfaces en los Sistemas de Gestión de Bases de Datos

Los sistemas de gestión de bases de datos (SGDB) que son una colección de programas que permiten a los usuarios crear y mantener una base de datos [2], es decir se puede ver como un programa de varios propósitos que facilita y permite desarrollar los pasos al definir, construir y manipular las bases de datos. Dicho software ofrece diferentes tipos de interfaz de acuerdo a las necesidades de los usuarios finales.

- Interfaces para la navegación de menús. Son listas de opciones desplegadas que evitan al usuario tener que memorizar instrucciones de consultas ya que van apareciendo nuevos submenús conforme va avanzando la complejidad de la consulta. Muy utilizados en sistemas de navegación.
- Interfaces basadas en formularios. Se refieren a un conjunto de campos que el usuario debe de llenar o modificar. Son específicos para cada sesión con el usuario, ya que cada vez que se desea ingresar datos a uno de estos es como si lo utilizaran por primera vez.
- Interfaces gráficas de usuario. Utiliza esquemas para su manipulación y consulta, con ayuda del Mouse se eligen las opciones deseadas y se puede acceder a un formulario elegido en dicho esquema.
- Interfaces del lenguaje natural. Interpretan solicitudes hechas por el usuario en lenguaje natural. Puede utilizar palabras reservadas para ayudar a la consulta. Si se tiene éxito se generará la consulta.
- Interfaces para usuarios paramétricos. Realizados para ambientes donde se tienen que hacer cierto número de transacciones repetitivas, para un conjunto reducido de usuarios, donde se pretende que las acciones que tenga que realizar sean la cantidad menos posible o tratar de generar procesos que se puedan realizar de manera automática.
- Interfaces para ABD. Se restringen instrucciones a un número muy reducido de empleados. Esto para mantener cierta seguridad en el ambiente de trabajo. Se puede implementar por medio de sesiones de trabajo por medio de nombres de usuario y contraseñas.

3 Generadores de Pantallas

Los lenguajes de tercera generación (3GL) necesitan de una gran cantidad de código para poder ejecutar un simple comando en contraposición con los 4GL que permiten hacer lo mismo con pocas líneas de código, los lenguajes de cuarta generación indican que debe de hacer el usuario y no como se debe de hacer. El usuario solo debe de indicar al sistema de generación de pantallas una serie de parámetros que se utilizarán para el despliegue de la aplicación, mejorando como se pretende acelerar el proceso de producción.

Dentro de los lenguajes de cuarta generación se encuentran, los ya citados lenguajes de consulta y generadores de informes, lenguajes especializados como hojas de cálculo y lenguajes de bases de datos, generadores de aplicaciones para el mantenimiento (IMEC) de bases de datos. Lenguajes de muy alto nivel para generar el código de la aplicación. [3]

Desde el punto de vista de los usuarios desarrolladores las interfaces descritas en los sistemas de gestión de bases de datos, los tipos de 4GL son:

- Generadores de formularios. El usuario puede definir el como se verá la pantalla, cuales datos quiere presentar en la pantalla y en donde desea que estos aparezcan, también se pueden incluir elementos de validación de datos, utilización de operadores aritméticos, entre otros.
- Generadores de informes. Extrae información de la base de datos y permite por medio de esta crear informes, la salida de la información debe ser bien definida, donde incluso hay algunas que permiten el despliegue con formularios previos.
- Generadores de gráficos. Pretende mostrar la tendencia de la información con datos extraídos de las bases de datos. donde esta la posibilidad de mostrar distintos tipos de gráficos.
- Generadores de aplicaciones. Funcionan como generadores de interfaces entre el usuario y las bases de datos. Como ya se ido mencionando reducen el tiempo de desarrollo de aplicaciones, todo esto se utiliza por medio de librerías previamente definidas. El usuario dice que se debe de hacer, el generador es quien dice como hacerlo.

4 Herramientas generadoras

Dentro de la gama de herramientas que pueden existir para generar ya sean informes, pantallas, reportes y consultas se pueden mencionar:

4.1 Microsoft Access

Permite generar por medio de un “wizard” formularios e informes. Para el caso de los formularios se hace mediante la selección de tablas que contienen los datos y dentro de cada tabla los campos deseados. Para el aspecto de presentación se pueden elegir diferentes opciones presentadas por el mismo, y varios aspectos que confieren al diseño del formulario. Permitiendo poder hacer un IMEC, jerarquizar otros formularios dependientes de uno principal, agregar botones con funcionalidades definidas y cuadros de texto para inclusión de información.

En cuanto a los informes, se da mediante a una serie de pasos similar a el de los formularios, los datos se pueden agrupar en diferentes niveles, según la prioridad indicada, como pertenece a la familia de Microsoft Office, permite la exportación del informe hacia un documento ya sea de Word o Excel

Para efectos de seguridad Microsoft Access ofrece distintas estrategias entre las cuales se pueden mencionar las siguientes [4]:

- *Restricción de acceso a usuario con opciones de inicialización:* Se pueden configurar de acuerdo al tipo de usuario restricciones al acceso a menús y barras de herramientas (ocultando las que no les sean permitidas), así como las bases de datos que pueda ver y acceso a teclas especiales. Esta estrategia se utiliza donde la seguridad muy estricta no es necesaria. También se puede combinar con otras estrategias de seguridad. La figura 1 muestra las opciones que deben restringirse.

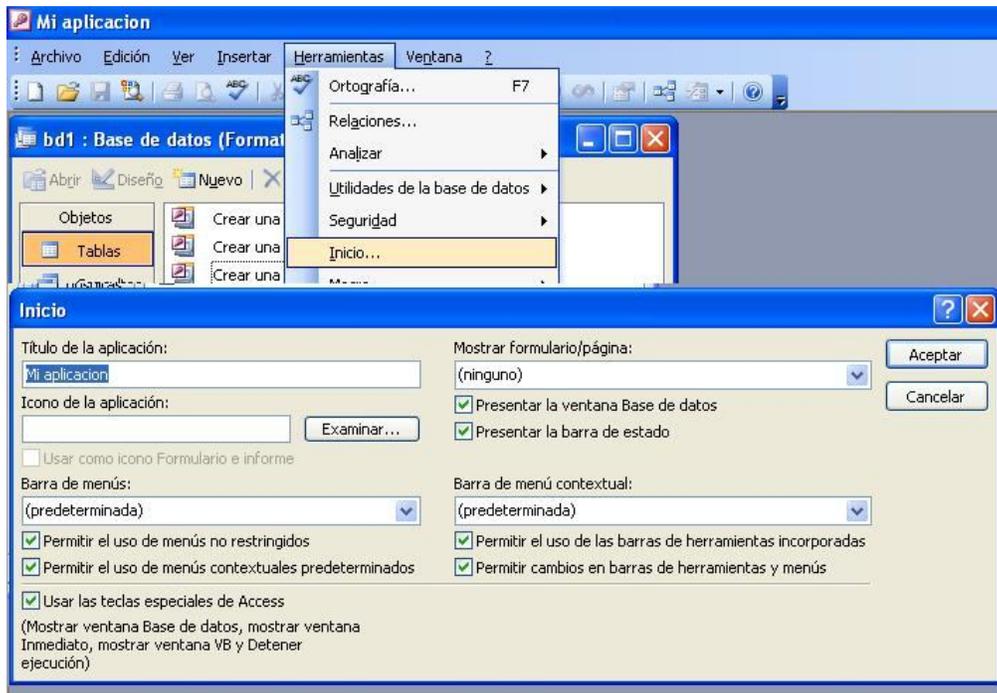


Figura 1. Restricción de acceso a usuarios al inicializar.

- **Protección de archivos abiertos:** Se asigna una clave de usuario para que solamente los usuarios permitidos puedan ver información de la base de datos. Se recomienda antes de asignarle contraseña a la base de datos hacer una copia de la misma y cerrarla. Si la base de datos se encuentra en un servidor o incluso en una carpeta compartida se debe asegurar que otro usuario no la tenga abierta. Para asignar la contraseña en la carpeta donde se tiene el archivo de la base de datos, se selecciona y se va a la pestaña ubicada en la parte inferior derecha llamada “abrir”, aquí se selecciona “Abrir en modo exclusivo”. Luego con el archivo abierto ya se puede asignar la contraseña según la figura 2.

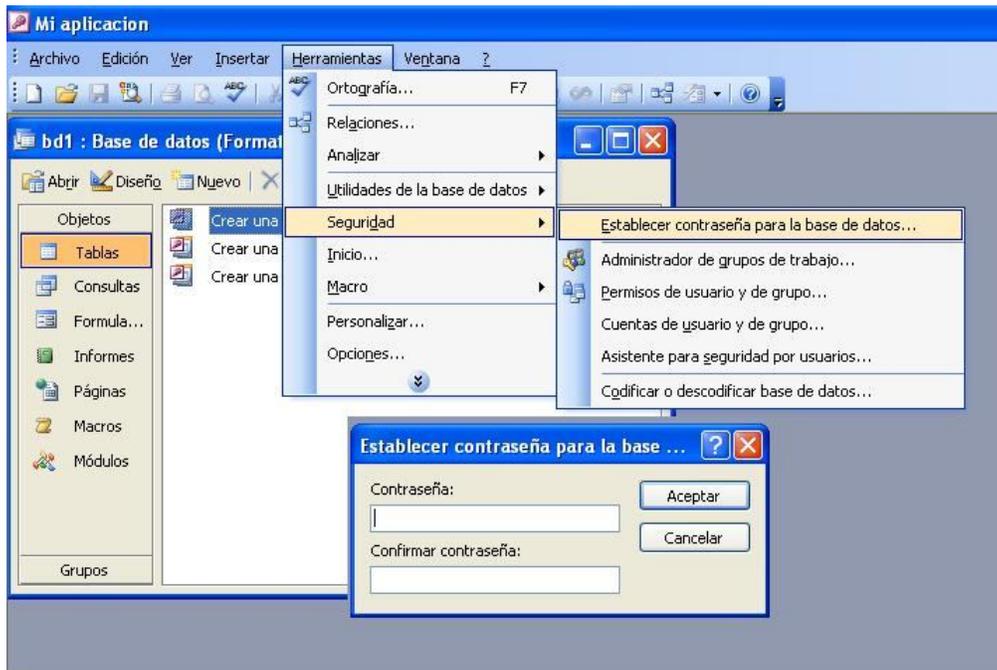


Figura 2. Protección de archivos abiertos.

- *Protección de código fuente:* Se puede grabar una aplicación como un archivo MDE con el fin de poder remover el código fuente que se encuentre escrito en Visual Basic (VBA) previniendo los cambios a formularios, reportes y módulos. Esta característica, encontrada partir de Access 97, lo que hace es copiar el contenido de los archivos MDB pero sin el código fuente del programa creado, permaneciendo la base de datos en estado compilado.
- *Encriptación de base de datos:* La encriptación permite que usuarios sin autorización no puedan acceder a ver la información de la base de datos.
- *Niveles de seguridad de usuario:* Agrega más fuerza y flexibilidad a los métodos de protección. Sin embargo, establecer niveles de seguridad a usuarios específicos es un proceso mucho más complejo que los demás y solamente desarrolladores más especializados la trabajan adecuadamente.

Como cualquier usuario que sepa la contraseña también puede limpiarla una vez que haya ingresado a la base de datos. Por defecto el creador de la base de datos, el grupo de usuarios y el grupo de administradores tienen permisos de administrador. Se pueden remover los permisos de administrador para los demás grupos y usuarios excepto para el administrador de la base de datos. Se pueden remover estos permisos (figura 3) sin utilizar seguridad por nivel de usuario pero los usuarios pueden restablecerse estos permisos por eso se hace estrictamente necesario crear estos niveles para evitar esta situación. Otra forma es utilizando el Editor de Política del Sistema que es un archivo llamado Poedit.exe y que activa políticas más fuertes para la seguridad. El mismo es una parte de la instalación del Office Resource Kit que se recomienda descargar actualizado cada cierto tiempo.



Figura 3. Permisos de administrador.

4.2 SPSS (Statistical Product and Service Solutions)

Actualmente SPSS aparte de representar el programa en sí también representa a la compañía que lo desarrolla. Este programa es utilizado para datos estadísticos, sobre todo en ciencias sociales y en mercadeo. Fue creado en 1968 por Norman H. Nie Hadlai Hull y Dale H. Bent. Permite realizar cálculos complejos de manera eficiente. A pesar de que el programa es eficaz en sus resultados no se debe de dejar de tomar en cuenta que la decisión de los datos al final reside en el usuario. Una de las ventajas presentadas es la generación de tablas cruzadas, que permiten mostrar los datos de una base de datos de una manera más resumida, es decir, clasificando la información y presentándola de forma agrupada en un reporte. Ver figura 4 con un ejemplo de reporte generado a partir de dos variables [5].

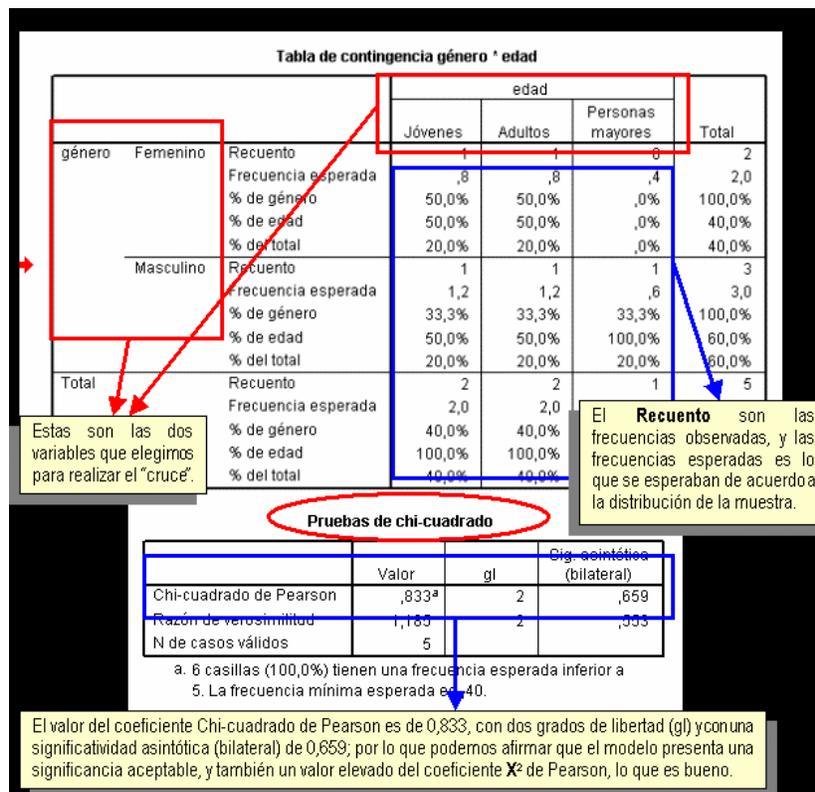


Figura 4. Reporte generado con SPSS

SPSS como compañía también desarrolló SmartViewer Web Server que un portal que sirve como intermediario entre el servidor de la base de datos y el cliente final. La gran ventaja que tiene es que se puede utilizar un navegador estándar sin necesidad de descargar plug-ins ni otra utilidad. Esta herramienta almacena los análisis creados en la organización, tablas pivot (permiten combinar diferentes variables, recorrido de información de lo general a específico, traslado de información de filas a columnas o viceversa, elaboración de gráficos), informes OLAP (el servidor permite resumir la información generando tablas más pequeñas con mayor cantidad de información recopilada), información contenida en html e incluso interactuar con archivos de Microsoft Excel[6].

La herramienta SmartViewer Web Server también permite restringir hacia quien va dirigida la información o quienes están permitidos para acceder a la información al poder categorizar los documentos. No utiliza informes estáticos sino más bien a partir de la información recopilada se pueden obtener informes actualizados en tiempo real utilizando los menús que tiene a su disposición. También utiliza XML desde que se están definiendo los datos hasta que se obtiene un documento final, esto lo hace convirtiendo las páginas Web en bases de datos categorizando diferentes tipos de datos, pudiéndose referenciar y utilizar en otros documentos.

4.3 RBase

Fue el primer programa para bases de datos relacionales para computadora, creado por Wayne Erickson in 1982, originalmente llamado MicroRIM (Relational Information Manager) desarrollado en Boeing Computer Service y utilizado por la NASA. Algunas de las opciones incluidas son un tutorial de desarrollo de aplicaciones para programación libre, capacidades de automatización multiusuario, opciones para lenguajes de cuarta generación, formularios, reportes, entre otros.

5 Seguridad en las Bases de Datos

Es claro que cuando se trata de información, siendo esta en este momento un recurso de vital importancia con el cual se pueden determinar patrones de comportamiento, es necesario proteger la información de accesos no deseados o restringir el uso de la misma dentro de los involucrados. Un buen sistema de administración de bases de datos debe de considerar resguardar y mostrar solo aquella que se solicita.

Cuando se habla de seguridad se deben de considerar varios aspectos referentes a la misma, accesos no autorizados, destrucción de información o modificación maliciosa de la misma o incluso la introducción de accidental de datos que pueden provocar inconsistencias. De estas es mucho más sencillo proteger al sistema contra las acciones de tipo accidental que las de índole malicioso. Los daños de tipo accidental incluyen alteración de la información por alguna circunstancia física. Existe por ello el concepto de unicidad de información, para evitar que los datos sean corrompidos por algún agente físico, el sistema manipula todo el paquete de datos como una unidad y por ende si alguno de los miembros de dicho paquete se corrompe toda la unidad también, esto provoca que no se guarde toda la información. También deben de contar con un sistema de recuperación de datos, por causas como pérdidas de información volátiles, interrupción de energía e incluso aquellos que provocan pérdida de información almacenada en disco duro. Por lo anterior toda transacción debe ejecutarse de manera atómica, la base de datos debe de estar en un estado consistente antes de ejecutar una transacción y después de que la finaliza. Los cambios no se verán reflejados hasta que termine de ejecutarse la transacción y su permanencia en el repositorio de la base.

Una transacción tiene dos formas de terminarse o correcta o incorrecta, en el caso de que finalice incorrectamente se deshace la transacción e incluso todos los cambios que pudo esta provocar en la base de datos

Hay que tener presente que la ética y aspectos legales de la información deben de considerarse en la publicación de la información, políticas corporativas definidas en cada empresa sujetas incluso a leyes constitucionales y diferentes niveles de seguridad definidos por ellos.

Hay dos mecanismos de seguridad que se pueden definir [7]:

- Discrecionales, otorgan privilegios a los usuarios
- Obligatorios, imponen seguridad en múltiples niveles clasificando los datos y los usuarios implementando las políticas de cada organización

Los mecanismos obligatorios se pueden hacer por medio de creación de perfiles (tipos de usuarios en el universo tratado) en las aplicaciones y luego la verificación de nombres de usuario y contraseñas, si por ejemplo, se observa que un usuario intenta el ingreso a un sistema en un número repetitivo de veces y no tiene éxito, el sistema de seguridad implantado en el software puede deducir que se intenta un acceso mal intencionado e incrementar la seguridad del mismo, o registrando en una bitácora este número de accesos, Windows Vista, el nuevo sistema operativo de la compañía Microsoft, cuenta con un control interno de restricciones para proteger los programas, archivos e incluso páginas web del acceso a los usuario de la computadora, además de bloquear dicho acceso, por cada vez que alguien intenta ingresar a un archivo se registra cual usuario fue y si persiste indica el número de intentos de ingreso.

Los llamados firewalls que protegen la computadora de accesos no deseados o malintencionados.

La encriptación de los mensajes es una forma de cifrar los datos hasta que lleguen a su destino. Este método permite autorizar a ciertos usuarios a encriptar y desencriptar los datos, para encriptar se necesita de una llave para poder hacerlo y otra para poder decodificarlo y un algoritmo de codificación.

En cuanto a las bases de datos que manipulan información estadística, los usuarios de las mismas están autorizados para obtener información a nivel general pero no sobre individuos específicos, incluso la elaboración de las consultas debe de hacerse de manera cuidadosa porque con base en esto se podría obtener hechos relativos a los individuos.

El administrador de la base de datos tiene funciones tales como crear nuevas cuentas, conceder y quitar privilegios y la asignación de los niveles de seguridad ya mencionados, dentro de los métodos para autorizar a los usuarios se pueden presentar los códigos y contraseñas, por medio de elementos bioatropométricos tales como voz, reconocimiento de retina, huellas dactilares, entre otros, información existente.

El refinamiento de la seguridad puede llegar a niveles tales que con el perfil de tipo de empleado se puede incluso bloquear un determinado campo de la base, o bien cierta función de la aplicación

SQL es un sistema administrador de bases de datos el cual permite el control de acceso discrecional, básicamente quien crea un objeto tiene todos los derechos sobre mismo, independientemente de las relaciones existentes se

pueden otorgar ciertos privilegios y generar ciertas relaciones u otra forma de hacerlo es otorgar los privilegios a las relaciones presentadas. También existen los bloqueos de tablas por medio de las vistas restringiendo privilegios a secciones de código.

Para mantener la integridad de la información y que los datos introducidos sean los que deben de ser, se tienen que tener presente que la validación, corrección y precisión se tienen que manipular en los procesos de IMEC, el sistema debe de corregir las operaciones incorrectas o por lo menos indicar que hay errores en estas, un acceso concurrente puede provocar cálculos de datos incorrectos, un ejemplo de ello puede ser al intentar modificar una tupla de dos terminales diferentes casi al mismo tiempo, los cálculos podrían hacerse en función de información incorrecta arruinando la integridad del dato.

Si bien a veces el sistema se queda inactivo una forma de protegerlo es sacar del sistema a usuarios con periodos de inactividad relativamente largos.

6 Conclusiones

Las bases de datos se han convertido en grandes almacenes de recursos y estos a su vez se han vuelto vulnerables a ataques por obtener dicho recurso. Es por ello que los sistemas administradores de bases de datos tienen que tener mecanismos de seguridad para poder manipular la información. En el mercado existen diferentes herramientas que hacen el proceso de generación de bases de datos muy sencillo y fácil de utilizar. El mediatismo del mundo actual obliga al desarrollo cada vez más rápido de sistemas lo cual provoca que la tecnología tenga que implementar una serie de procesos para poder simplificar ciertas tareas en el desarrollo de pantallas, formularios e informes.

Referencias

[1] [2] Elmasri R.A. Fundamentos de Sistemas de bases de Datos. Tercera Edición, España: Addison Wesley. 2004.

[3] <http://www3.uji.es/%7Emmarques/f47/apun/node38.html>

[4] <http://office.microsoft.com/en-us/ork2000/CH011492851033.aspx>

[5] <http://www.aulafacil.com/investigacionsspss/Lecc-21.htm>

[6] <http://www.spss.com/es/pdf/svws.pdf>

[7] <http://209.85.165.104/search?q=cache:WLkHAqzN-vMJ:alarcos.inf-cr.uclm.es/doc/adbd/docs/AdBD-T3.pdf+Seguridad+%2B+bases+de+datos&hl=es&ct=clnk&cd=9&gl=cr&client=firefox-a>