24021
33

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

ACATLAN

IMPLEMENTACION DE UN SISTEMA DE CONTROL DE SEGURIDAD EN BASE DE DATOS

TRABAJO DE SEMINARIO
TALLER EXTRACURRICULAR
QUE PARA OBTENER EL TITULO DE
LICENCIADO EN MATEMATICAS
APLICADAS Y COMPUTACION
P R E S E N T A
RUBICEL MEDINA GOMEZ

ASESOR: LIC. JUAN TORRES LOVERA

Dirección General de Bibliotecas
...fundir en formato electrónico e im...
...de mi trabajo re...
...RE: Rubicel Medina Gómez
...A: 02/JUL/2003
...MA:

JULIO 2003

TESIS CON
FALLA DE ORIGEN

A

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Gracias a:

Mis profesores de seminario:

LIC. GERARDO ROLDÁN CEVALLOS.
ACT. HUGO REYES MARTÍNEZ.
M. en A. IGNACIO MARTÍN LIZÁRRAGA GAUDRY.
LIC. JUAN TORRES LOVERA.
ACT. LUZ MARÍA LAVÍN ALANÍS.

Sin ellos no hubiera sido posible la realización de éste trabajo.

A mis padres:

Como una forma de agradecimiento por todos sus esfuerzo y por el cariño y apoyo que siempre me han brindado.

A mis Hermanos:

Por ayudarme en cuanto han podido y por darme su ejemplo en su desempeño profesional.

A mi esposa Josefina y a mi hijo Daniel Axel:

Gracias por quererme y apoyarme, ustedes son la razón para seguir adelante.

"Los amo"

TESIS CON
FALLA DE ORIGEN

INDICE

TESIS CON
FALLA DE ORIGEN

Introducción

La razón de implementar un sistema de control de seguridad en bases de datos, obedece a que la seguridad en la informática es un tema que toma cada vez más importancia, tanto en el ámbito mundial como en el país.

El avance de la tecnología da lugar a que el procesamiento de la información sea más fácil, sin embargo, es necesario tomar nuevas medidas en cuanto a la implementación de los sistemas informáticos para que los usuarios de los sistemas, no puedan acceder a información que no les pertenece.

Uno de los problemas más graves que trae consigo el avance tecnológico, es la seguridad. Los países industrializados y los que no los son, requieren cada vez más el uso de la tecnología informática. Esta necesidad se ha vuelto una amenaza al bienestar económico, a la seguridad ciudadana, y a la seguridad nacional de muchos países, aún de los más poderosos. Cabe señalar que, la menaza va en aumento, y que por lo tanto se demanda a gente capacitada y de investigación de nuevas tecnologías.

La parte medular de los sistemas de información es el almacenamiento de datos. Existen dos enfoques para el almacenamiento de datos en un sistema basado en computadora. El primer método es guardar los datos en archivos individuales, cada uno de ellos único para cada aplicación particular. El segundo enfoque para el almacenamiento de datos en un sistema basado en computadora involucra la construcción de una base de datos. Una base de datos es un almacén de datos formalmente definido y centralmente controlado para ser usado en muchas aplicaciones diferentes, es decir es una fuente central de datos que está pensada para que sea compartida por muchos usuarios con una diversidad de aplicaciones.[1]

El presente trabajo se enfocará a la seguridad en las bases de datos, ya que éstas son en donde se realizan mayor número de transacciones y procesamiento de la información.

Cualquier sistema de base de datos, deberá ser valorado, fundamentalmente por la seguridad que brinde, ya que uno de los principales objetivos es poner a disposición de la mayor cantidad de personas al interior de una organización, la información procesada. Esto será factible, sólo si se planifican desde el comienzo del diseño de sistemas medidas que garanticen un acceso ágil y seguro a la información clasificada como pública. Adoptar nuevas medidas de seguridad a un sistema, luego de que ha ocurrido alguna violación o falla cuando éste ya ha sido implementado (como sucede en la mayoría de los casos) puede traer como consecuencia una mala relación costo-efectividad de los controles. Para que esto no ocurra, desde las etapas preliminares del diseño, se debe cerciorar que se tomen las medidas necesarias para implementar la seguridad en todos y cada uno de los componentes del sistema.

El acceso público a la información clasificada como tal, es algo que, en función de los recursos tecnológicos y de comunicaciones de los que se disponen hoy día, no tendría que ser objeto de ningún tipo de limitaciones. Sin embargo, si todo el entorno informático no está preparado para

[1] Kendall & Kendall, "Análisis y Diseño de Sistemas", Prentice Hall (3ra Edición-1997) Pág. 585, 588

TESIS CON
FALLA DE ORIGEN

ese cometido desde el punto de vista de auditoria y seguridad, es muy difícil llevar adelante este objetivo.

Los elementos a tener en cuenta en seguridad referente a la administración del personal encargado de operar los sistemas de información y de los usuarios en general están relacionados con las interacciones de las personas, los equipos informáticos y las autorizaciones que cada uno necesita para llevar a cabo su trabajo. Para ello los cuatro puntos que se consideran fundamentales para esta tarea son:

- Organización del Personal.
- Administración de Usuarios.
- Permisos de accesos del personal contratado.
- Accesos Públicos.

Se puede afirmar que los controles de acceso a la información constituyen uno de los parámetros más importantes a la hora de administrar seguridad. Con ellos determinamos quién puede acceder a qué datos, indicando a cada persona un tipo de acceso (perfil) específico. Para este cometido se utilizan diferentes técnicas que se diferencian significativamente en términos de precisión, sofisticación y costos. Se utilizan por ejemplo, palabras claves, algoritmos de encriptación, listas de controles de acceso, limitaciones por ubicación de la información, horarios, etc.

Una vez determinados los controles de accesos a la información, se hace imprescindible efectuar una eficiente administración de la seguridad, lo que implica la implementación, seguimiento, pruebas y modificaciones sobre los "Perfiles" de los usuarios de los Sistemas. Este es uno de los puntos fundamentales a tener en cuenta para garantizar la seguridad y al mismo tiempo una correcta accesibilidad a la información. A lo largo del trabajo de investigación, se propone un control de la seguridad de la información, apoyándose en un sistema de control de accesos.

En todo proyecto informático que pretenda brindar información a diferentes niveles, garantizando correcta toma de decisiones y accesibilidad a un amplio espectro de usuarios, se deberá prestar mucha atención a este punto. Para ello es importante que se plantee en la organización, la necesidad de establecer estándares para la administración de seguridad de accesos. Con ello se garantizará un eficiente, seguro y al mismo tiempo correcto uso de la información.

A lo largo del trabajo de investigación, se propone un control de la seguridad de la información, apoyándose en un sistema de control de accesos. Este sistema no solo comprende desarrollar un control de accesos a la base de datos ni un programa que haga usuarios ni perfiles de acceso, o auditar una base de datos, por el contrario también comprende elaborar una serie de políticas y programas para tener un correcto control en la seguridad de la información enfocada a una base de datos.

La política de auditoria y seguridad informática debe formar parte de los lineamientos generales a desarrollarse, sobre la base de las directivas emanadas de la gerencia general y formará parte del compromiso de ésta en su aplicación. En ella se deberá establecer con claridad y precisión las metas a alcanzar y las responsabilidades asignadas.

TESIS CON
FALLA DE ORIGEN

Asimismo se estudiará con sumo cuidado las facilidades que el sistema de base de datos ofrezca para su auditabilidad, qué tipo de información genera, con qué facilidad se pueden definir opciones, etc. Un aspecto que merecerá también la atención en el trabajo de investigación será el control de acceso que posea, la posibilidad de definición y grupos de perfiles. Más aún usando un procesamiento distribuido será objeto de nuestra atención el procesamiento y replicación segura, como así también todo mecanismo que garantice la integridad de los datos en forma automática.

Las decisiones relacionadas con la seguridad informática no son triviales. Muchas veces no se sabe por donde empezar, ¿cómo conseguir un nivel de seguridad?, ¿Cómo saber sise tiene un nivel mínimo de seguridad?, ¿Qué beneficio habrá si se define un plan de contingencia?. En muchas organizaciones, estas responsabilidades recaen sobre una única persona, quien implícitamente las aplica sin una definición formal. Este hecho implica importantes conflictos, dado que los diferentes grupos o personas no entienden o no interpretan de la misma forma los conceptos necesarios; y esto, por lo tanto, puede impedir tomar decisiones críticas de forma satisfactoria en situaciones de emergencia.

Es por eso que en el presente trabajo, se abordarán estos temas por medio de la siguiente organización:

- En el capítulo uno, se verán antecedentes de la seguridad informática; así como los conceptos básicos relacionados con las bases de datos y las características de los sistemas de control para la seguridad en bases de datos.

- En el capítulo dos, se revirará la planeación de la seguridad en base de datos en las organizaciones, además se estudiará la metodología empleada para implantar el sistema de control de seguridad y la forma en como es usado para determinar el análisis y diseño del sistema. Así mismo, se indica en éste capítulo, el manual de operación administrativo para controlar y proveer los accesos a los sistemas.

- Finalmente, en el capítulo tres, se abordarán los resultados del sistema de control de seguridad a partir de la reingeniería de software, y por lo tanto se revisará el análisis costo - beneficio del sistema. Finalmente se comentará la escalabilidad y prospectiva del sistema.

TESIS CON
FALLA DE ORIGEN

Objetivo General

Elabora el proceso de asignación de aplicaciones y privilegios mediante el diseño de un sistema que tenga una interfaz gráfica para la asignación de los mismos y así poder controlar la seguridad en la base de datos.

Objetivos particulares

- Ayudar a crear una conciencia de la importancia de la seguridad informática.
- Conocer las diferentes formas de vulnerar la seguridad de los sistemas y las técnicas empleadas para solucionar éstas deficiencias.
- Poner de manifiesto la necesidad y justificación de protección de la información almacenada en las bases de datos
- Que el lector adquiera un grado de análisis y pueda planificar una política de seguridad, analizando los riesgos de exposición del sistema y conozca las medidas de solución existentes.
- Introducir al lector en las técnicas, herramientas y procedimientos de protección de la información en las bases de datos.

Como resultado de esta investigación y de acuerdo a lo planeado, se deberá estar en la posibilidad de llegar a conclusiones propias acerca de la importancia que se le debe de otorgar al tema de la seguridad de la información en las bases de datos apoyándose de un sistema integro de control de seguridad, dentro de cada una de las diversas organizaciones, ya sean de carácter educativo o empresarial.

TESIS CON
FALLA DE ORIGEN

PAGINACIÓN DISCONTINUA

CAPÍTULO I

LA SEGURIDAD EN LA INFORMACIÓN Y SU SITUACION EN LOS SISTEMAS DE BASES DE DATOS

. **Objetivo:**

Explicar el origen y la importancia de la seguridad en la información, además de los antecedentes de las bases de datos relacionales y los problemas a que se enfrentan los "Administradores de las Bases de Datos" en la tarea de asignar aplicaciones y privilegios a los usuarios de un sistema que tiene como plataforma una base de datos, así como la desventaja al no poder supervisar las transacciones que se hacen al sistema. Esta problemática dará pie a que se reconozca la ventaja de automatizar el proceso de asignación de aplicaciones y privilegios, y de poder llevar un control de quien, que día y a que hora, realizo una transacción determinada.

TESIS CON
FALLA DE ORIGEN

1.1 Antecedentes de la Seguridad en la Información

Desde que el ser humano tiene conciencia, la información ha tenido gran importancia en cualquier actividad. Cuando la información tiene propósitos muy especiales, como el militar o el personal, la información crece en importancia y requiere mayor atención en su resguardo. La información, como elemento indispensable en la comunicación, se puede calificar en varios niveles dependiendo su valor; por ejemplo, existe información confidencial en las actividades militares, en las actividades comerciales importantes, en las transacciones financieras, etc., una forma de poder dar seguridad a toda esta información es implementar y usar diversos métodos de control de acceso a ella.

Los delitos informáticos comenzaron a surgir desde la invención de los primeros sistemas de cómputo. En aquella época, para que se diera un incidente de seguridad, el delincuente tenía que estar directamente desde la terminal del sistema, por lo que se reducía el índice de probabilidad de que dicho ataque pudiera venir de personas de afuera o no pertenecientes a las empresas o ambientes académicos

Las bases de datos empleadas en los sistemas de cómputo son herramientas muy poderosas que desde hace unos años han adquirido una importancia insospechada. Se ha llegado a depender de las computadoras como nunca antes se hizo de ningún otro dispositivo electrónico, pues gran parte de los datos que almacenan son usados para el procesamiento de transacciones, que de otra forma llevaría mucho tiempo en realizarse.

Por consecuencia, la seguridad en las tecnologías de la información, se convierte en, un tema de crucial importancia para el continuo y espectacular progreso de la sociedad, e incluso para su propia supervivencia. Motivo por el cual se hace de vital necesidad establecer políticas y lineamientos de acceso a estos dispositivos que manipulan y almacenan datos de relevada importancia para la mayoría de las personas actualmente.

El enemigo más común para los sistemas de cómputo es nosotros mismos, y las causas que obligan a cometer tales delitos, se pueden dividir en dos grupos:

Mayor Riesgo:

- Beneficio personal
- Odio a la organización
- Mentalidad turbada
- Equivocación de ego
- Deshonestidad del departamento
- Problemas financieros de algún individuo
- Fácil modo de desfalco

Menor Riesgo:

- Beneficio de la organización
- Jugando a jugar

TESIS CON
FALLA DE ORIGEN

Los avances tecnológicos que día a día se van logrando, no se han mantenido distantes del mundo de la informática, por el contrario han ido a la par y constantemente se van logrando avances significativos que hacen posible tener computadoras más sofisticadas, equipos de cómputo mejores, redes de cómputo más veloces, etc. Hace tan solo 20 años cuando las computadoras aún no estaban conectadas unas con otras y el Internet era solo un proyecto de unos cuantos, era prácticamente difícil creer en incidentes de seguridad. Por el año de 1983, nació el protocolo de comunicación TCP/IP que trajo consigo una posible comunicación entre sistemas de cómputo, las distancias se acortaron, los sistemas de cómputo cambiaron de ser siempre redes de área local (LAN) se extendieron a uso metropolitano (MAN) e incluso alcance mundial (WAN); surgió la tendencia Cliente – Servidor, los sistemas de cómputo se unieron y comenzó la integración del mundo gracias a la tecnología y a las redes de computadoras. En ese entonces no se pensaba en individuos que pudieran acceder a sistemas de cómputo remotos y mucho menos pensar que pudieran causar daño desde distancias lejanas. Con el paso del tiempo, cada vez fue más notable lo inseguro que eran los sistemas y que tanto hardware como software contenían fallas de elaboración y de programación respectivamente.

Los primeros incidentes de seguridad llegaron, y con ellos múltiples problemas; pero no había legislación, no existía algún organismo que fuera el responsable de denunciarlos ni que pudiese hacer algo al respecto. En aquellos años a finales de los 80's la mayoría de los crackers utilizaban técnicas tan triviales como el adivinar el login (clave de acceso) y de saber el nombre del usuario, tratar de penetrar el sistema con contraseñas fáciles de adivinar, siendo ésta una tarea trivial y que hoy en día aún la practican.

Posteriormente surgieron grandes incidentes de seguridad en el ámbito mundial; por ejemplo, entre los hechos criminales más famosos están:

- El caso del Banco Wells Fargo donde se evidencio que la protección de archivos era inadecuada, cuyo error costo USD 21.3 millones.
- El caso de la NASA donde dos alemanes ingresaron en archivos confidenciales.
- El caso de un muchacho de 15 años que entrando a la computadora de la Universidad de Berkeley en California destruyo gran cantidad de archivos.
- También se menciona el caso de un estudiante de una escuela que ingreso a una red canadiense con un procedimiento de admirable sencillez, otorgándose una identificación como un usuario de alta prioridad, y tomo el control de una embotelladora de Canadá.
- También el caso del empleado que vendió la lista de clientes de una compañía de venta de libros, lo que causo una perdida de USD 3 millones
- El 28 de diciembre de 1998 un grupo de hackers norteamericanos, la "Legión of the Underground", declaro la "ciberguerra" contra Irak y China, amparándose en que en ambos países no se respetan los derechos y libertades fundamentales, llamaron a la destrucción masiva de todas las redes informáticas de estos países. Su primera víctima fue el servidor oficial del gobierno Iraquí, que sucumbió el 7 de enero.

Estos hechos y otros nos muestran claramente que los componentes del sistema de información no presentaban un adecuado nivel de seguridad. Ya que el delito se cometió con y sin intención. Donde se logró penetrar en el sistema de información.

TESIS CON
FALLA DE ORIGEN

Es muy importante manejar con discreción los resultados que se obtengan de los aspectos de seguridad, pues su mala difusión podría causar daños mayores. Esta información no debe ser divulgada y se la debe mantener como reservada.

Sin embargo, el resto de la comunidad de hackers[1], se opone frontalmente a este tipo de medidas. En el manifiesto que estos otros grupos publicaron, declamaron "oponerse totalmente a cualquier intento de usar el poder del hacking para amenazar o destruir las infraestructuras de comunicación de cualquier país", por cuanto "las redes de comunicaciones son el sistema nervioso de nuestro planeta". También, a raíz del bombardeo de la embajada de china en Belgrado (mayo 1999), los internautas chinos inundaron la red con consignas en contra de Estados Unidos, entraron en la web de la embajada estadounidense y colapsaron las charlas en directo, condenando las acciones de la Alianza.

Este tipo de situaciones dieron pauta a la creación del máximo organismo de Seguridad en los Estados Unidos, y en 1988 se creo el CERT (Computer Emenrgency Response Team), al cual se unieron el FIRST (Forum of Incident and Response Security Teams), y la CIAC (Computer Incident Advisory Capabilities).

También se dio la creación de sucursales de equipos de respuesta a los Incidentes de Seguridad en casi la mayoría de los países que no estaban aislados a los cambios tecnológicos constantes como lo fue en 1995 la creación en nuestro país de la sucursal del CERT, llamado MX-CERT. Se comenzaba a hacer conciencia de que había un problema y que dicho problema ocasionaba perdidas millonarias en empresas tanto privadas como gubernamentales, siendo su principal punta de lanzamiento los ambientes académicos y de ahí perpetrar a las industrias privadas, bancos, institutos de investigación, etc.

Desgraciadamente casi ninguna institución tiene políticas ni procedimientos, nadie sabe qué es permitido, ni qué es prohibido. Es muy alarmante encontrar que salvo las grandes corporaciones , la normatividad relativa a la tecnología de información es prácticamente inexistente; no hay lineamientos establecidos para administrar recursos como el correo electrónico, los mecanismos de seguridad, los niveles de servicio en redes y la atención de problemas.

La cultura de la seguridad informática es entonces un concepto que debe cubrir todos los niveles jerárquicos de la organización, así como todas las funciones que la conforman.

[1] Persona que disfruta con la exploración de los detalles de los sistemas programables y cómo aprovechar sus posibilidades; al contrario de la mayoría de los usuarios, que prefieren aprender solo lo imprescindible ("The New Hacker's Dictionary", Segunda Adición, de Eric S. Raymond

TESIS CON
FALLA DE ORIGEN

1.2 Importancia de la Seguridad Informática en las Empresas.

Seguridad Informática

No existe una definición estricta de lo que se entiende por seguridad informática, puesto que ésta abarca múltiples y muy diversas áreas relacionadas con los sistemas de información. Áreas que van desde protección física de la máquina como componentes de hardware de su entorno; hasta la protección de la información que contiene, o de las redes que lo comunican con el exterior.

Tampoco es único el objetivo de la seguridad. Son muy diversos tipos de amenazas contra los que se debe proteger; desde amenazas físicas, como los cortes eléctricos, hasta errores no intencionados de los usuarios, pasando por los virus informáticos o el robo, destrucción o modificación de la información.

El reconocimiento de la necesidad de seguridad es una conclusión natural de la creencia de que la información es un recurso organizacional fundamental. Debe hacerse notar que conforme más gente de la organización obtenga mayor poder de cómputo, la seguridad llega a ser cada vez más difícil y compleja.

La seguridad tiene tres aspectos interrelacionados: física, lógica y de comportamiento. Los tres deben de trabajar juntos si se pretende que la calidad de que la calidad de la seguridad permanezca alta.

Seguridad física.- La seguridad física se refiere a la seguridad de las instalaciones de computación, su equipo y software por medios físicos. Esto puede incluir el control del acceso al cuarto de la computadora por medio de gafetes legibles por máquina o sistemas de registro/despedida humanos, el uso de cámaras de televisión de circuito cerrado para monitorear las áreas de computadora y el respaldo de datos frecuentemente así como el almacenamiento de los respaldos en un área a prueba de fuego y agua.

Seguridad lógica.- La seguridad lógica se refiere a los controles lógicos del mismo software. Los controles lógicos familiares para la mayoría de los usuarios son contraseñas y códigos de autorización de algún tipo. Cuando son usados permiten que el usuario con la contraseña correcta entre al sistema o a una parte particular de la base de datos.

Seguridad del comportamiento.- La seguridad puede comenzar por investigar a los empleados que actualmente tendrán acceso a las computadoras, datos e información, para asegurarse de que sus intereses sean consistentes con los de la organización y que comprenden completamente la importancia de llevar acabo procedimientos de seguridad.

Existen circunstancias en las que además de desplegar las tecnologías de seguridad más avanzadas, la confidencialidad de los datos obliga a tomar medidas adicionales para garantizar la legitimidad de los accesos. Este es, por ejemplo, el caso de números de tarjetas de créditos, información financiera o datos de carácter personal.

TESIS CON
FALLA DE ORIGEN

Cada vez existen más empresas y organizaciones preocupadas por la seguridad de su información en las bases de datos e inversiones tecnológicas, pero muy pocas realizan un estudio en profundidad de la seguridad de sus sistemas, identificación de elementos a proteger, análisis de vulnerabilidades, y establecimientos de prioridades. Cuando se habla de la función informática generalmente se tiende a hablar de tecnología nueva, de nuevas aplicaciones, nuevos dispositivos hardware, nuevas formas de elaborar información más consistente, etc. Sin embargo se suele pasar por alto o se tiene muy implícita la base que hace posible la existencia de los anteriores elementos. Esta base es la información.

Es muy importante conocer su significado dentro la función informática. Entendemos por *información* el conjunto de datos que sirven para tomar una decisión. La información también es necesaria para el estudio de las desviaciones y de los efectos de las acciones correctoras; es un componente vital para el control. El manejo de información generada por computadora difiere en formas significativas del manejo de los datos producidos manualmente. Por lo general, hay mayor cantidad de información de computadora a administrar. El costo de organizarla y mantenerla puede crecer a tasas alarmantes, y los usuarios la tratan menos escépticamente que la información obtenida por otras vías.[3] De tal forma, cuando la información esta basada en tecnología, tiene las siguientes características:

- Esta almacenada y procesada en computadoras.
- Puede ser confidencial para algunas personas o a escala institucional.
- Puede ser mal utilizada o divulgada.
- Puede estar sujeta a robos, sabotaje o fraudes.

Los primeros puntos nos muestran que la información esta centralizada y que puede tener un alto valor y los últimos puntos nos muestran que se puede provocar la destrucción total o parcial de la información, que incurre directamente en su disponibilidad que puede causar retrasos de alto costo. Una de las razones principales que explica la falta de inversión en seguridad en las empresas (tanto en estudios como en sistemas) es que éstas no cuantifican correctamente el riesgo de una intrusión o incidente en seguridad, y por lo tanto no valoran (o consideran justificada) una inversión en sistemas de protección.

Los siguientes puntos identifican algunos de los daños que puede afectar una violación en la seguridad de la información de un sistema[4]:

- Datos e información que dejan de estar disponibles
- Pérdida de productividad
- Daños en la imagen corporativa
- Pérdidas totales por cada fallo o incidente
- Pérdidas en los años siguientes

Pensemos por un momento que se sufre un accidente en el centro de computo o el lugar donde se almacena la información. Ahora preguntémonos: ¿Cuánto tiempo pasaría para que la

[3] Kendall & Kendall, "Análisis y Diseño de Sistemas", Prentice Hall (3ra Edición-1997) Pág. 1
[4] John G. Burch, Jr. Felix R. Strater Jr. "Sistemas de Información Teoría y Práctica", Ed. Limisa 5ta Edición 1986 Pág. 379

TESIS CON
FALLA DE ORIGEN

organización este nuevamente en operación?. Es necesario tener presente que el lugar donde se centraliza la información con frecuencia el centro de cómputo puede ser el activo más valioso y al mismo tiempo el más vulnerable.

Para continuar es muy importante conocer el significado de dos palabras, que son riesgo y seguridad.

Riesgo

Proximidad o posibilidad de un daño, peligro, etc.
Cada uno de los imprevistos, hechos desafortunados, etc., que puede cubrir un seguro.
Sinónimos: amenaza, contingencia, emergencia, urgencia, apuro.

Seguridad

Cualidad o estado de seguro
Garantía o conjunto de garantías que se da a alguien sobre el cumplimiento de algo.
Ejemplo: Seguridad Social Conjunto de organismos, medios, medidas, etc., de la administración estatal para prevenir o remediar los posibles riesgos, problemas y necesidades de los trabajadores, como enfermedad, accidentes laborales, incapacidad, maternidad o jubilación; se financia con aportaciones del Estado, trabajadores y empresarios.
Se dice también de todos aquellos objetos, dispositivos, medidas, etc., que contribuyen a hacer más seguro el funcionamiento o el uso de una cosa: cierre de seguridad, cinturón de seguridad.

Con estos conceptos claros se puede decir que la criminología ya ha calificado los "delitos hechos mediante computadora" o por "sistemas de información" en el grupo de delitos de cuello blanco.

- **Tipos de Delitos**

Los delitos cometidos utilizando la computadora han crecido en tamaño, forma y variedad. En la actualidad los delitos cometidos tienen la peculiaridad de ser descubiertos en un 95% de forma casual. Podemos citar a los principales delitos hechos por computadora o por medio de computadoras estos son:

- Fraudes.
- Falsificación.
- Venta de información.

En la actualidad se nota que los fraudes crecen en forma rápida, incluso mayor que los sistemas de seguridad. Se sabe que en los EE.UU. se cometen crímenes computarizados denunciados o no por más de 3 mil millones de dólares.). Por esto es importante conocer las causas para que se cometan delitos, ya que una vez encontrado el problema se debe observar la raíz para sugerir su solución. Además al ingresar al área de seguridad se debe contemplar muy estrechamente las relaciones que hay entre los aspectos: tecnológicos, humano - sociales y administrativos.

TESIS CON
FALLA DE ORIGEN

Costo por pérdida de información

Se debe evaluar las aplicaciones y la dependencia del sistema de información, para lo cual es importante considerar responder las siguientes cuatro preguntas:

1. ¿Qué sucedería si no se puede utilizar el sistema? Si el sistema depende de la aplicación por completo se debe definir el nivel de riesgo.
Por ejemplo citemos:

- Un sistema de reservación de boletos que dependa por completo de un sistema computarizado, es un sistema de alto riesgo.
- Una lista de clientes será de menor riesgo.
- Un sistema de contabilidad fuera del tiempo de balance será de mucho menor riesgo

2. ¿Qué consecuencias traería si es que no se pudiera acceder al sistema? Al considerar esta pregunta se debe cuidar la presencia de manuales de respaldo para emergencias o algún modo de cómo se soluciono este problema en el pasado.

3. ¿Existe un procedimiento alternativo y que problemas ocasionaría? Se debe verificar si el sistema es único o es que existe otro sistema también computarizado de apoyo menor. Ejemplo: Sí el sistema principal esta diseñado para trabajar en red sea tipo WAN quizá haya un soporte de apoyo menor como una red LAN o monousuario. En el caso de un sistema de facturación en red, si esta cae, quizá pudiese trabajar en forma distribuida con un módulo menor monousuario y que tenga la capacidad de que al levantarse la red existan métodos de actualización y verificación automática.

4. ¿Qué se ha hecho en casos de emergencia hasta ahora? Para responder esta pregunta se debe considerar al menos las siguientes situaciones, donde se debe rescatar los acontecimientos, las consecuencias y las soluciones tomadas, considerando

- Que exista un sistema paralelo al menos manual
- Si hay sistemas duplicados en las áreas críticas (tarjetas de red, teclados, monitores, servidores, unidades de disco, aire acondicionado)
- Si hay sistemas de energía interrumpida UPS.
- Si las instalaciones eléctricas, telefónicas y de red son adecuadas (se debe contar con el criterio de un experto).
- Si se cuenta con un método de respaldo y su manual administrativo.

Cuando se ha definido el grado de riesgo se debe elaborar una lista de los sistemas con las medidas preventivas que se deben tomar y las correctivas en casi de desastre, señalando la prioridad de cada uno. Con el objetivo que en caso de desastres se trabajen los sistemas de acuerdo a sus prioridades.

Ahora que se han establecido los riesgos dentro la organización, se debe evaluar su impacto a nivel institucional, para lo cual se debe:

- Clasificar la información y los programas de soporte en cuanto a su disponibilidad y recuperación.

TESIS CON
FALLA DE ORIGEN

- Identificar la información que tenga un alto costo financiero en caso de perdida o pueda tener impacto en el ámbito ejecutivo o gerencial.
- Determinar la información que tenga un papel de prioridad en la organización a tal punto que no pueda sobrevivir sin ella.

Una vez determinada esta información se la debe CUANTIFICAR, para lo cual se debe efectuar entrevistas con los altos niveles administrativos que sean afectados por la suspensión en el procesamiento y que cuantifiquen el impacto que podrían causar estas situaciones.

Disposiciones que Acompañan la Seguridad

De acuerdo a experiencias pasadas, y a la mejor conveniencia de la organización, desde el punto de vista de seguridad, contar con un conjunto de disposiciones o cursos de acción para llevarse a cabo en caso de presentarse situaciones de riesgo. Para lo cual se debe considerar:

- Obtener una especificación de las aplicaciones, los programas y archivos de datos.
- Medidas en caso de desastre como perdida total de datos, abuso y los planes necesarios para cada caso.
- Prioridades en cuanto a acciones de seguridad de corto y largo plazo.
- Verificar el tipo de acceso que tiene las diferentes personas de la organización, cuidar que los programadores no cuenten con acceso a la sección de operación ni viceversa.
- Que los operadores no sean los únicos en resolver los problemas que se presentan.

Higiene

Otro aspecto que parece de menor importancia es el de orden e higiene, que debe observarse con mucho cuidado en las áreas involucradas de la organización (centro de computo y demás dependencias), pues esto ayudará a detectar problemas de disciplina y posibles fallas en la seguridad. También podemos ver que la higiene y el orden son factores que elevan la moral del recurso humano, evita la acumulación de desperdicios y limita las posibilidades de accidentes. Además es un factor que puede perjudicar el desarrollo del trabajo tanto a nivel formal como informal.

Cultura Personal

Cuando hablamos de información, su riesgo y su seguridad, siempre se debe considerar al elemento humano, ya que podría definir la existencia o no de los más altos grados de riesgo. Por lo cual es muy importante considerar la idiosincrasia del personal, al menos de los cargos de mayor dependencia o riesgo.

El fin de este punto es encontrar y evitar posibles situaciones de roce entre el recurso humano y la organización logrando así una mejor comunicación entre ambos.

TESIS CON
FALLA DE ORIGEN

1.3 Breve Historia e Introducción a las Bases de Datos Relaciónales

Base de Datos

Con el paso de los años, ha habido muchas definiciones de base de datos, pero en forma sencilla, una base de datos es una colección organizada de datos que sirven para un objetivo central. Está organizada en el sentido de que contiene datos que están almacenados, tienen un formato, son accesibles y están representados de manera coherente.

Sirve para un objetivo central en el sentido de que no contiene datos externos o superfluos. Frecuentemente, el objetivo de una base de datos es un negocio, pero podría almacenar datos científicos, militares o de otro tipo, normalmente datos de empresa. De ahí que haya bases de datos de empresa, científicas, militares, etc.

Al hablar de bases de datos y diseño de bases de datos en particular, es habitual hacer referencia al objetivo central al que sirve una base de datos, su ocupación, sea cual sea su campo más específico, que puede ser aerospacial, biomédico, o cualquier otro. [5]

Introducción a DBMS

Un sistema de gestión de bases de datos (DBMS, *Database ManageMent System*) es el software que gestiona (administra) una base de datos. Actúa como un repositorio para todos los datos y es responsable de su almacenamiento, seguridad, e integridad, simultaneidad, recuperación y acceso. El DBMS tiene un diccionario de datos, al que se conoce como el catálogo del sistema, que almacena datos sobre todo lo que contiene, como nombres, estructuras, ubicaciones y tipos.

L a seguridad siempre es una preocupación en la base de datos de producción. Normalmente no se suele plantear el hecho de qué tipo de seguridad disponer, sino cuánta. Normalmente un DBMS ofrece varias capas de seguridad además del sistema operativo y de las instalaciones de seguridad de la red. Frecuentemente, un DBMS contiene cuentas de usuarios con contraseñas que requieren que el usuario se conecte, o sea autenticado, para acceder a la base de datos.

El DBMS también ofrece otros mecanismos, como grupos, roles, privilegios y perfiles, que ofrecen te forma conjunta un mayor refinamiento en la seguridad. Estos niveles de seguridad no sólo permiten la ejecución, sino también el establecimiento de políticas de seguridad de empresa.

Comunicación con la base de datos

Un DBMS no es bueno si no se puede comunicar con él. A las bases de datos se puede acceder a través de un lenguaje de acceso o de consulta. El lenguaje de consultas estructurado (SQL Structured Query Language) es el lenguaje de consultas que predomina actualmente.

---

[5] William G. Page, Jr. "Oracle8/8i", Ed Prentice Hall, Edición Especial 1999 Pág. 5

Toda la comunicación a y desde la base de datos debe pasar a través del DBMS, y para esto, se utiliza SQL. El modelo relacional fue presentado por Codd de la empresa IBM a fines de los años 60. Antes de nacer los RDBMS como DB2, existían modelos jerárquicos y de red. Antes de estos modelos, las bases de datos se creaban utilizando archivos planos y rutinas de acceso de lenguaje.[6]

Una base de datos relacional no es más que un conjunto de relaciones que contienen la información almacenada en la base de datos.

Objetivos del modelo relacional

Independencia Física

Es decir, que el modo en que se almacenan los datos no influya en su manipulación lógica y, por tanto, los usuarios que acceden a esos datos no tengan que modificar sus programas por cambios en el almacenamiento físico.

Independencia Lógica

Esto es, que el añadir, eliminar o modificar objetos de la base de datos no repercuta en los programas y/o usuarios que están accediendo a subconjuntos parciales de los mismos.

Flexibilidad.- En el sentido de poder presentar a cada usuario los datos de la forma en que éste prefiera.

Uniformidad.- Las estructuras lógicas de los datos presentan un aspecto uniforme, lo que facilita la concepción y manipulación de la base de datos por parte de los usuarios

Sencillez.- Las características anteriores, así como unos lenguajes de usuario muy sencillos, producen como resultado que el modelo de datos relacional sea fácil de comprender y de utilizar por parte del usuario final

Relación(tablas)

La relación(tabla), es la estructura básica del modelo. Todos los datos de una base de datos se representan en forma de relaciones cuyo contenido varía en el tiempo. Formalmente una relación es un conjunto de filas en terminología relacional.

Para la manipulación de estas tablas(dinámica), se propone un conjunto de operadores. Alguno de ellos clásicos de la teoría de conjuntos y otros introducidos por el modelo relacional. Estos operadores forman el álgebra relacional.

Existe una serie de términos utilizados en el modelo relacional que se definen:

[6] William G. Page, Jr, "Oracle8/8i", Ed Prentice Hall, Edición Especial 1999 Pág. 9

Relación.- Conjunto de filas. Puede asociarse a lo que se conoce como tabla, con ciertas propiedades.

Tupla.- Corresponde a una fila de esa tabla. Al número de tuplas se denomina cardinalidad.

Atributo.- Se refiere a una columna de esa tabla. La cantidad de atributos determina el grado de la relación.

Definiciones relacionales

Clave Primaria.-identificador único para la tabla. Se compone de una columna o de una combinación de ellas. Nunca existen dos filas de la misma tabla con el mismo valor de la clave primaria.

Dominio.- Es una colección de valores, de los cuales uno o más atributos obtienen sus valores reales. Se define dominio como "un conjunto de valores escalares de donde extraen sus valores los atributos de una relación". Los valores escalares representan la menor unidad semántica de información. Los dominios tienen una importancia semántica, puesto que restringen las comparaciones. Los dominios no sólo definen los valores permitidos, sino además las comparaciones permitidas.

Relaciones.- La cabecera está compuesta por un conjunto fijo de atributos, o en términos más precisos de pares atributos-dominio :
{ (A1:D1), (A2:D2), ..,(An:Dn)} tales que cada atributo Aj corresponde a uno y solo uno de los dominios subyacentes Dj.
Una relación R, sobre un conjunto de dominios D1,D2,..,Dn (no necesariamente todos distintos), se compone de dos partes, una cabecera y un cuerpo.
El cuerpo está formado por un conjunto de tuplas, el cual varía con el tiempo. Cada tupla está compuesta por un conjunto de pares atributo-valor :
{ (A1:v1), (A2:v2), ..,(An:vn)} para cada una de estas tuplas hay uno de estos pares atributo valor.

Propiedades de las relaciones

Las propiedades de las relaciones son un consecuencia de su definición:

- No existen tuplas repetidas . Por tratarse, el cuerpo de una relación, de un conjunto matemático estos no admiten elementos repetidos. Como corolario aparece la clave primaria.
- Las tuplas no están ordenadas (de arriba hacia abajo).
- Los atributos no están ordenados (de izquierda a derecha)
- Todos los valores de los atributos son atómicos. Es equivalente a decir las relaciones no contienen grupos repetitivos y en este caso estarían normalizadas.

TESIS CON
FALLA DE ORIGEN

Tablas Base Son tablas creadas vía un comando del lenguaje de definición de datos, los datos asociados a estas tablas son almacenados permanentemente en memoria secundaria. Tablas Derivadas Constituyen derivaciones de las tablas básicas, obtenidas mediante la utilización de comandos de un lenguaje de manipulación de datos. Los datos de este tipo de tabla tienen una vida temporal y normalmente constituyen datos redundantes.

Vistas

Las vistas también se denominan tablas virtuales. Las tuplas que compondrán las vistas serán generadas cada vez que la vista requiera ser utilizada.
Los datos que componen una vista provienen de la ejecución de algunos comandos del lenguaje de manipulación de datos.
Para crear una vista se utiliza un algoritmo especialmente definido para este fin, el cual es ejecutado cada vez que se utiliza la vista y es almacenado en memoria secundaria, este procedimiento es absolutamente transparente ara el usuario.
Existen dos razones principales para utilizar Vistas:

- Calcular valores en función de datos almacenados en las tablas de la base.
- Restringir acceso tanto a filas como columnas de una tablas para determinados usuarios.

Reglas de Integridad

El modelo relacional define dos reglas generales para mantener la integridad de los datos :

- Integridad de la entidad : Una clave primaria no puede aceptar valores nulos.
- Integridad de las referencias : Todo valor definido como clave foránea debe tener su correspondencia con un valor de clave primaria en la relación referenciada.

Base de Datos Relacional

Conociendo los conceptos antes presentados, podemos definir una base de datos relacional como "un conjunto de relaciones normalizadas de distinto grado".

-El modelo relacional es uno de los modelos de bases de datos más utilizados y que presenta una fuerte base teórica.
-Existe una gran variedad de Sistemas Administradores de Bases de Datos en el mercado, basados en este modelo: Oracle, SyBase, Informix, Ingres, DB2, entre otros.
-El modelo relacional suele dividirse en tres partes :

- Estructura de datos (Relación)
- Integridad
- Manipulación

TESIS CON
FALLA DE ORIGEN

Lenguaje de Datos Relacional

El modelo relacional considera un lenguaje de datos que permite la definición y manipulación de datos. La porción de lenguaje de manipulación de datos (DML) permite la obtención de información (consultas), mediante operadores de consulta que se basan en el álgebra relacional. A su vez, el lenguaje de definición de datos (DDL) permite la definición de esquemas relacionales (Creación de tablas, vistas, privilegios, etc.).[7]

Álgebra Relacional

El álgebra relacional consiste en un conjunto de operadores de alto nivel que operan sobre relaciones. Cada uno de estos operadores toma una o dos relaciones como entrada y produce una nueva relación de salida.

Codd define un conjunto de ocho operadores clasificados en dos grupos:

a) Las operaciones tradicionales de conjuntos unión, intersección, diferencia y producto cartesiano.
b) Los operadores especiales de restricción, proyección reunión y división.

Unión: Construye una relación formada por todas las tuplas que aparecen en cualquiera de las dos relaciones especificadas

Intersección :Construye una relación formada por aquellas tuplas que aparezcan en las dos relaciones especificadas

Diferencia: Construye una relación formada por todas aquellas tuplas de la primera relación que no aparezcan en la segunda de las dos relaciones especificadas

Producto cartesiano: A partir de dos relaciones especificadas, construye una relación que contiene todas las combinaciones posibles de tuplas, una de cada una de las relaciones.

Restricción: Extrae las tuplas especificadas de una relación dada (restringe la relación solo a las tuplas que satisfagan una condición especificada)

Proyección: Extrae los atributos especificados de una relación dada

Reunión: A partir de dos relaciones especificadas, construye una relación que contiene todas las posibles combinaciones de tuplas, una de cada una de las dos relaciones, tales que las dos tuplas participantes en una combinación dada satisfagan alguna condición especificada

División: Toma dos relaciones, una binaria y una unaria y construye una relación formada por todos los valores de una atributo de la relación binaria que concuerdan (en el otro atributo) con todos los valores de la relación unaria.

[7] Glenn A. Jackson "Introducción al Diseño de Bases de Datos Relacionales" Ed. Prentice-Hall, Pág.3

TESIS CON
FALLA DE ORIGEN

Lenguaje de Consulta Estructurado (SQL)

SQL (Structured Query Language) es un lenguaje que permite la definición y la manipulación de una base de datos relacional. Se ha establecido como el lenguaje estándar de bases de datos relacionales, utilizándose en la mayoría de los SABDR como Oracle, Informix, Sybase, DB2, SQLServer, etc. Aunque las versiones de SQL utilizadas en productos difiere en aspectos del lenguaje, podría hablarse de la existencia de un estándar. Las Bases de Datos Relacionales se han convertido en la forma principal de almacenamiento en la mayoría de los sistemas comerciales, ya que permiten almacenar y accesar un gran volumen de información de una forma sencilla y rápida; en donde el usuario debe tener un conocimiento del lenguaje de interrogación para accesar a estos datos, en general SQL (Structure Query Language).[8]

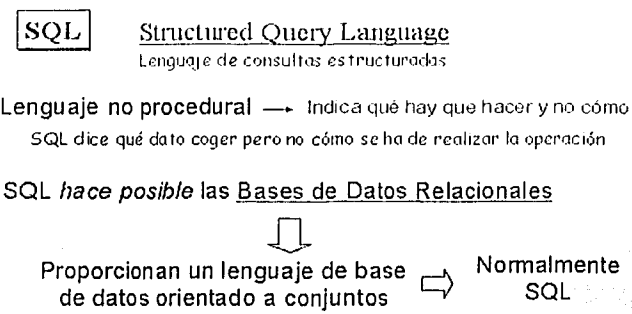


Fig. 1.1 Lenguaje estructurado de base de datos

SQL se puede usar en forma interactiva o inmerso en lenguajes de programación de propósito general como Cobol, C , Power Builder, Visual Basic, etc.
SQL se compone de :

- DDL (lenguaje de definición de datos) : Define y modifica esquemas relacionales, crear tablas, crear vistas, definir accesos, etc.
- DML (lenguaje de manipulación de datos) : Basado en el álgebra relacional permite la recuperación de información.

La estructura de una consulta simple en SQL es :

SELECT : Lista los atributos deseados.
FROM : Lista las tablas que se van a utilizar en la consulta.

[8] S.M Deen. "Fundamentos de los sistemas de bases de datos", Ed. Gustavo Gili, S.A., Barcelona 1987. Pág. 177

WHERE : Consta de un predicado que implica atributos de las relaciones que aparecen en la cláusula FROM.

Otras cláusulas de SQL:

INSERT : Inserta una nueva fila (tupla) en la tabla.
Insert Into nombre_tabla (atributo1, atributo2,...)
Values (valor1, valor2, ...);

UPDATE : Actualiza valores de atributo de una tabla.
Update nombre_tabla
Set atributo = valor
Where condición;

DELETE : Elimina tuplas de la tabla que cumplan con la condición.
Delete
From nombre_tabla
Where condición;

GRANT : Concede privilegios de acceso a los datos a los usuarios.
Grant privilegio On Table nombre_tabla
To identificación_usuario;

Diseño de base de datos

Una de las formas de diseñar una base de datos relacional es comenzar con un modelo E/R. El modelo entidad relación es un modelo semántico de datos, por lo que debe ser "refinado" para que corresponda a los formalismos de un sistema administrador de base de datos relacional.

Del modelo E/R modelo Relacional

El paso de un esquema en el modelo ER al modelo relacional está basado en los tres principios siguientes:

- Toda Entidad se convierte en una relación.
- Toda interrelación N:M se transforma en una relación.
- Toda interrelación 1:N se traduce en el fenómeno de propagación de claves o se crea una nueva relación.

Normalización

La teoría de normalización apoya el diseño de bases de datos relacionales buscando una forma más deseables para las relaciones del modelo (en términos de mantener la integridad). Se dice que una relación está en una determinada forma normal si satisface un cierto número de restricciones. El modelo relacional considera como obligatoria sólo la Primera Forma Normal, las formas normales superiores persiguen un fin de optimización.

Otros Modelos de Bases de Datos

Los sistemas de bases de datos pueden clasificarse de acuerdo a las estructuras de datos y a los operadores presentados al usuario. Entre los sistemas más antiguos se encuentran los modelos de Red y Jerárquicos (prerrelaciónales). Uno de los modelos más importantes es el Modelo Relacional aparecido en los 70. Posteriormente aparecen los llamados sistemas postrelacionales entre los se cuentan:

- Sistemas Relacional Extendido
- Sistemas Orientados a Objeto
- Sistemas Deductivos

El modelo relacional se presenta como uno de los modelos más utilizados para la construcción de bases de datos. Su poderío se centra en que utiliza una sola estructura de datos, la relación, lo que le otorga gran flexibilidad, uniformidad y sencillez. SQL es el lenguaje estándar de las SABDR y permite definir y manipular tablas , siendo utilizado tanto en forma interactiva como inmerso en aplicaciones. Las bases de datos relacionales y las tecnologías de bases de datos orientadas a objetos se espera que cada vez más soporten el acceso a –y la construcción de- recursos críticos de conocimiento organizacional, no sólo datos altamente estructurados. En las manos de diseñadores imaginativos, la tecnología de bases de datos relacionales puede proporcionar muchas de las funciones primitivas de la administración del conocimiento, incluyendo separar contenido y las relaciones en un ambiente en red que soporta múltiples usuarios control concurrente y cambio rápido y continuo.

1.4 Sistemas de Control para la Seguridad en Base de Datos.

Para entender de mejor forma los sistemas computacionales, primeramente se define lo que es un sistema. Un sistema es un conjunto de partes coordinadas para lograr un conjunto de metas[9]. Los sistemas involucran los siguientes aspectos:

1.- Los objetivos del sistema considerados como un todo y más específicamente las medidas de actuación del sistema completo.
2.- El medio ambiente del sistema: las restricciones fijas.
3.- Los recursos del sistema: las restricciones fijas.
4.- Los componentes del sistema, sus actividades, metas y medidas de actuación
5.- La administración del sistema.

En el sentido más estricto, los sistemas son: "Una serie de elementos que forman una actividad, un procedimiento o un plan de procesamiento que buscan una o más metas en común en una referencia de tiempo, mediante la manipulación de datos, información, energía o materia para obtener al final información, energía o materia." Un Sistema Administrador de Base de Datos (SABD) es una colección de programas que permite a los usuarios crear y mantener una base de datos. En estos sistemas administradores de bases de datos una de las funciones más importantes es de proveer la seguridad en la información.

[9] C. West Churchman "El enfoque de sistemas". Ed. Diana México 1968 Pág. 47

La importancia de almacenar, manipular y recuperar la información en forma eficiente ha llevado al desarrollo de una teoría esencial para las bases de datos. Esta teoría ayuda al diseño de bases de datos y procesamiento eficiente de consultas por parte de los usuarios.

El área de Administración de la base de datos es el área encargada de velar porque los modelos de datos y los sistemas de información que funcionan sean consistentes, correctos, seguros y se puedan acceder de una forma rápida y confiable mediante construcción de índices, constraints y otras técnicas de bases de datos.

La persona encargada de administrar la base de datos además de asignar privilegios sobre la información tiene las siguientes funciones:

- Entender la arquitectura de los manejadores de bases de datos utilizados en la organización.
- Garantizar el correcto funcionamiento de las bases de datos.
- Definir perfiles de usuario, otorgar privilegios, matricular usuarios.
- Definir estrategias de manejo de los discos.
- Diseñar el sistema de backups de la base de datos.
- Dimensionar las bases de datos y crear la base de datos.
- Afinar la base de datos, optimizando su desempeño y tiempo de respuesta.
- Instalar nuevas versiones de los manejadores de bases de datos que posee la institución.
- Asesorar a los analistas en el diseño del modelo de datos de cada sistema de información.
- Cuidar la integridad del modelo de datos corporativo.
- Establecer mecanismos para garantizar la seguridad de los datos almacenados en la base de datos.
- Crear, mantener y analizar indicadores de gestión del área.

Consideraciones para Elaborar un Sistema de Seguridad Integral

Como hablamos de realizar la evaluación de la seguridad es importante también conocer como desarrollar y ejecutar el implantar un sistema de seguridad.

Desarrollar un sistema de seguridad significa: "planear, organizar coordinar dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad física de los recursos implicados en la función informática, así como el resguardo de los activos de la empresa."

Por lo cual podemos ver las consideraciones de un sistema de integral de seguridad.

Sistema Integral de Seguridad

Un sistema integral debe contemplar:

- Definir elementos administrativos
- Definir políticas de seguridad
  - A nivel departamental
  - A nivel institucional
- Organizar y dividir las responsabilidades
- Contemplar la seguridad física contra catástrofes (incendios, terremotos, inundaciones, etc.)
- Definir prácticas de seguridad para el personal:
  - Plan de emergencia (plan de evacuación, uso de recursos de emergencia como extinguidores.
  - Definir el tipo de pólizas de seguros
  - Definir elementos técnicos de procedimientos
  - Definir las necesidades de sistemas de seguridad para:
  - Hardware y software
  - Flujo de energía
  - Cableados locales y externos
- Aplicación de los sistemas de seguridad incluyendo datos y archivos
- Planificación de los papeles de los auditores internos y externos
- Planificación de programas de desastre y sus pruebas (simulación)
- Planificación de equipos de contingencia con carácter periódico
- Control de desechos de los nodos importantes del sistema:
- Política de destrucción de basura copias, fotocopias, etc.
- Consideración de las normas ISO 14000

Etapas para Implementar un Sistema de Seguridad

Para dotar de medios necesarios para elaborar su sistema de seguridad se debe considerar los siguientes puntos:
-Sensibilizar a los ejecutivos de la organización en torno al tema de seguridad.
-Se debe realizar un diagnóstico de la situación de riesgo y seguridad de la información en la organización a nivel software, hardware, recursos humanos, y ambientales.
-Elaborar un plan para un programa de seguridad. El plan debe elaborarse contemplando:

Plan de Seguridad Ideal (o Normativo)

Un plan de seguridad para un sistema de seguridad integral debe contemplar:

- El plan de seguridad debe asegurar la integridad y exactitud de los datos
- Debe permitir identificar la información que es confidencial
- Debe contemplar áreas de uso exclusivo
- Debe proteger y conservar los activos de desastres provocados por la mano del hombre y los actos abiertamente hostiles
- Debe asegurar la capacidad de la organización para sobrevivir accidentes

- Debe proteger a los empleados contra tentaciones o sospechas innecesarias
- Debe contemplar la administración contra acusaciones por imprudencia

Un punto de partida será conocer como será la seguridad, de acuerdo a la siguiente ecuación.

$$\text{SEGURIDAD} = \frac{\textbf{Riesgo}}{\textbf{Medidas preventivas y correctivas}}$$

Donde:
Riesgo (roles, fraudes, accidentes, terremotos, incendios, etc)
Medidas preventivas. (políticas, sistemas de seguridad, planes de emergencia, plan de resguardo, seguridad de personal, etc)

La Privacidad de la Información

El valor de la información depende directamente de la privacidad y utilidad que ésta tenga. La ecuación que relaciona esto podrá ser de la siguiente manera:

$$\textbf{VI} = \textbf{(P*U)/100\%}$$

DONDE

P=PRIVACIDAD

U=UTILIDAD

VI=VALOR DE LA INFORMACION

Consideraciones para con el Personal

Es de gran importancia la elaboración del plan considerando el personal, pues se debe llevar a una conciencia para obtener una auto evaluación de su comportamiento con respecto al sistema, que lleve a la persona a:

- Asumir riesgos
- Cumplir promesas
- Innovar

Para apoyar estos objetivos se debe cumplir los siguientes pasos:

Motivar
Se debe desarrollar métodos de participación reflexionando sobre lo que significa la seguridad y el riesgo, así como su impacto en el ámbito empresarial, de cargo y individual.

Capacitación General
En un principio a los ejecutivos con el fin de que conozcan y entiendan la relación entre seguridad, riesgo y la información, y su impacto en la empresa. El objetivo de este punto es que se podrán detectar las debilidades y potencialidades de la organización frente al riesgo.
Este proceso incluye como práctica necesaria la implantación la ejecución de planes de contingencia y la simulación de posibles delitos.

Capacitación de Técnicos
Se debe formar técnicos encargados de mantener la seguridad como parte de su trabajo y que esté capacitado para capacitar a otras personas en lo que es la ejecución de medidas preventivas y correctivas.

Ética y Cultura
Se debe establecer un método de educación estimulando el cultivo de elevados principios morales, que tengan repercusión en el ámbito personal e institucional.

Etapas para Implantar un Sistema de Seguridad en Marcha

Para hacer que el plan entre en vigor y los elementos empiecen a funcionar y se observen y acepten las nuevas instituciones, leyes y costumbres del nuevo sistema de seguridad se deben seguir los siguiente 8 pasos:

1. Introducir el tema de seguridad en la visión de la empresa.
2. Definir los procesos de flujo de información y sus riesgos en cuanto a todos los recursos participantes.
3. Capacitar a los gerentes y directivos, contemplando el enfoque global.
4. Designar y capacitar supervisores de área.
5. Definir y trabajar sobre todo las áreas donde se pueden lograr mejoras relativamente rápidas.
6. Mejorar las comunicaciones internas.
7. Identificar claramente las áreas de mayor riesgo corporativo y trabajar con ellas planteando soluciones de alto nivel.
8. Capacitar a todos los trabajadores en los elementos básicos de seguridad y riesgo para el manejo del software, hardware y con respecto a la seguridad física.

Conclusiones Capítulo I

En la sección 1.1 se a hecho ver que desde que se usa la computadora como instrumento de almacenamiento, procesamiento y transmisión de la información, mejora en gran medida el desempeño de las organizaciones, pero esto ha traído consigo nuevos retos, como es el de la protección de los datos a todos los niveles de la organización.

Para remarcar la problemática de la protección de la información usando la computadora, se hizo un breve recuentro de incidentes en seguridad en el ámbito mundial. Una vez teniendo una visón general de los antecedentes de la seguridad informática se menciona en el apartado 1.2 la importancia de la seguridad informática en las empresas, y se concluye que la información basada en la tecnología puede tener un valor incalculable y a su vez puede ser destruida parcial o totalmente.

Para el manejo de información centralizada a gran escala se ha implementado el uso de diversas técnicas y herramientas, una de la más importantes, son las bases de datos relacionales, su nacimiento, ha dado lugar a desarrollar lenguajes para el manejo de las mismas y el uso de modelos estructurales de relación de datos, es decir el modelo relacional, estos temas son tratados en la sección1.3, aquí se remarca el uso del lenguaje estructurado de base de datos (SQL), y su relación con el sistema de gestión, éste tema ayuda a comprender la forma en como se puede proteger la información en una base de datos.

Por último en el apartado 1.4 se estudia la definición de los sistemas administradores de base de datos, y los requerimientos con que debe de contar para su correcto funcionamiento. Después de haber hecho un recuento de la historia y las técnicas que sirven para manipular la información usando la tecnología, se concluye que la falta de cultura en seguridad informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, por lo que cada vez se requieren mayores conocimientos en tecnologías de la información las cuales permitan tener u marco de referencia aceptable para el manejo de dichas situaciones.

Bibliografía, Capítulo I

- Eric S. Raymond, "The New Hacker's Dictionary" Segunda Edición 1996

- Kendall & Kendall, "Análisis y Diseño de Sistemas", Prentice Hall 3ra Edición-1997

- William G. Page, Jr, "Oracle 8/8i" , Ed. Prentice Hall, Edición Especial 1999

- S.M. Deen. "Fundamentos de los sistemas de bases de datos", Ed. Gustavo Gili, S.A., Barcelona 1987

- Glenn A. Jackson "Introducción al Diseño de Base de Datos Relacionales" Ed. Prentice-Hall

- John G. Burch, Jr, Felix R. Strater Jr. "Sistemas de información Teoría y Práctica", Ed. Limusa 5ta Edición 1986

- C. West Churchman "El enfoque de sistemas para la toma de decisiones" Ed. Diana México 1973

CAPÍTULO II

DESARROLLO DEL SISTEMA DE CONTROL DE SEGURIDAD

. **Objetivo:**

Una vez haciendo el análisis de la problemática y las ventajas al implementar el sistema de accesos, en el **Capítulo II** se elaborará el "Desarrollo" de dicho sistema, que estará basado en la metodología "Yourdon". Esta metodología incluye un "Análisis Preliminar", que es un enfoque global de las funciones que la aplicación requiere para operar, así mismo mediante la metodología "Yourdon", se estructura el flujo de la información y la forma en como se guarda esta en la base de datos. Y por último se detalla cada uno de los procesos que componen a todo el sistema.

2.1 Planeación para el desarrollo de la seguridad

Planear la seguridad de la información almacenada en base de datos en uno de los aspectos más delicados en el ciclo de vida de un sistema y es uno de los aspectos que se le da menos prioridad, como ya se menciono en el capítulo I.

En el campo de la naturaleza de la planeación, el sistema global para el control de la seguridad, hasta cierto punto es una planeación estratégica, porque las políticas entorno al acceso de la información y el diseño del sistema de seguridad en base de datos, pretende que sea a largo plazo, pero el sistema que acompaña el control de accesos a la base de datos, por los avances tecnológicos es una planeación táctica, ya que los juicios tomados en ésta planeación, fueron seleccionar la infraestructura tecnológica.

Las organizaciones que cambian su infraestructura de seguridad en la información, tienen una orientación estratégica y esto lleva a que su tipo de planeación sea preactivista, es decir, se basa en pronósticos del comportamiento de los usuarios de los sistemas, de la competencia, así como de las condiciones económicas sociales y políticas de la organización.

Además en este tipo de organizaciones se piensan que la tecnología es la principal causa de cambio, y tratan de hacerlo lo más rápido posible, es decir, están a la vanguardia en avances tecnológicos.

La planeación preactiva consta de dos partes, *predicción* y *preparación,* además se inicia en el nivel más alto de una organización con la preparación de uno o más propósitos para el futuro. "La efectividad de la planeación preactiva depende de la precisión de los pronósticos para los que se prepara".[10]

Algunos de los aspectos que se planean antes de implantar un sistema que administra la seguridad de información en una base de datos es:

- Evaluar el ambiente de seguridad actual
- Alinear la solución de seguridad con los objetivos del negocio
- Proporcionar un informe con una recomendación acerca de la solución de seguridad que debería implementar la empresa.

Una vez que se han identificado las soluciones de seguridad específica para la empresa, se debe de diseñar una arquitectura de seguridad empresarial para proteger la información corporativa esencial. Este proceso incluye el diseño y desarrollo de una arquitectura completa pero flexible, que define los objetivos generales de diseño y operación para la seguridad, continuidad y el control de los recursos de información.

Además se debe considerar que a medida que se implementen nuevas medidas de seguridad y las necesidades de la empresa cambian y crecen, es importante efectuar evaluaciones periódicas de su solución de seguridad para continuar operando a un nivel de efectividad máximo.

[10] Rusell L. Ackoff "El paradigma de Ackoff Una administración Sistémica" Ed. Limusa primera Edición. Pág. 109

Como menciona Ackoff en el libro "El arte de resolver problemas": 'Pocos problemas, una vez resueltos, permanecen así; las condiciones cambiantes tienden a dejar sin solución a problemas que ya la tenían.'[11]

Las tareas para la implementación de un sistema de seguridad no deben terminar en que este operando el sistema sino también se deben de efectuar los siguientes puntos:

- Documentar el ambiente de seguridad
- Entrenar al personal interno en la administración y manejo del nuevo ambiente
- Realizar evaluaciones periódicas

La metodología empleada para implementar la seguridad a desarrollar es estrategia para proteger la disponibilidad, integridad y confidencialidad de los datos de los sistemas informáticos de las organizaciones. Además es útil para los administradores de recursos de información, los directores de seguridad informática y los administradores, y tiene un valor especial para todos aquellos que intentan establecer directivas de seguridad. La metodología ofrece un acercamiento sistemático a esta importante tarea y, como precaución final, también implica el establecimiento de planes de contingencia en caso de desastre.

Los datos de los sistemas informáticos están en constante peligro por varias causas: errores de los usuarios o ataques intencionados o fortuitos. Pueden producirse accidentes y ciertas personas con intención de atacar el sistema pueden obtener acceso al mismo e interrumpir los servicios, inutilizar los sistemas o alterar, suprimir o robar información.

Los sistemas informáticos pueden necesitar protección en algunos de los siguientes aspectos de la información:

- Confidencialidad. El sistema contiene información que requiere protección contra la divulgación no autorizada. Por ejemplo, datos que se van a difundir en un momento determinado (como, información parcial de informes), información personal e información comercial patentada.
- Integridad. El sistema contiene información que debe protegerse de modificaciones no autorizadas, imprevistas o accidentales. Por ejemplo, información de censos, indicadores económicos o sistemas de transacciones financieras.
- Disponibilidad. El sistema contiene información o proporciona servicios que deben estar disponibles puntualmente para satisfacer requisitos o evitar pérdidas importantes. Por ejemplo, sistemas esenciales de seguridad, protección de la vida y predicción de huracanes.

Para desarrollar éste sistema de seguridad de información, se debe de planear el tiempo, dinero y esfuerzo que hay que invertir para desarrollar las directivas y controles de seguridad apropiados. Cada organización debe analizar sus necesidades específicas y determinar sus requisitos y limitaciones en cuanto a recursos y programación.

[11] Russell L. Acoff, "El arte de resolver problemas." Ed..Limusa Pág. 229

Cada sistema informático en su entorno y directiva organizativa es distinto, lo que hace que cada servicio y cada estrategia de seguridad sean únicos. Sin embargo, los fundamentos de una buena seguridad siguen siendo los mismos

Aunque una estrategia de seguridad puede ahorrar mucho tiempo a la organización y proporcionar importantes recomendaciones de lo que se debe hacer, la seguridad no es una actividad puntual. Es una parte integrante del ciclo vital de los sistemas. Las actividades que se deben hacer para darle mantenimiento al sistema suelen requerir actualizaciones periódicas o las revisiones correspondientes.

Estos cambios se realizan cuando las configuraciones y otras condiciones y circunstancias cambian considerablemente o cuando hay que modificar las leyes y normas organizativas. Éste es un proceso iterativo. Nunca termina y debe revisarse y probarse con periodicidad.

El establecimiento de un conjunto eficaz de directivas y controles de seguridad requiere el uso de un método para determinar los puntos vulnerables que existen en nuestros sistemas y en las directivas y controles de seguridad que los protegen.

El estado actual de las directivas de seguridad informática se puede determinar mediante la revisión de la siguiente lista de documentación. La revisión debe tomar nota de las áreas en las que las directivas son deficitarias y examinar los documentos que haya:

- Directiva de seguridad informática física, como los controles de acceso físico.
- Directivas de seguridad de la red (por ejemplo, las referentes al correo electrónico y a Internet).
- Directivas de seguridad de los datos (control de acceso y controles de integridad).
- Planes y pruebas de contingencias y de recuperación de desastres.
- Conocimiento y formación en seguridad informática.
- Directivas de administración y coordinación de la seguridad informática.

Otros documentos que contienen información importante como:

- Contraseñas del BIOS de los equipos.
- Contraseñas para la configuración de enrutadores.
- Documentos de control de acceso.
- Otras contraseñas de administración de dispositivos.

Identificar métodos, herramientas y técnicas de ataque probable

Las listas de amenazas, de las que disponen la mayoría de las organizaciones, ayudan a los administradores de seguridad a identificar los distintos métodos, herramientas y técnicas de ataque que se pueden utilizar en los ataques. Los métodos pueden abarcar desde virus y gusanos a la adivinación de contraseñas y la interceptación del correo electrónico. Es importante que los administradores actualicen constantemente sus conocimientos en esta área, ya que los nuevos métodos, herramientas y técnicas para sortear las medidas de seguridad evolucionan de forma continua.

TESIS CON
FALLA DE ORIGEN

Establecer planes proactivos y reactivos

En cada método, el plan de seguridad debe incluir una estrategia proactiva y otra reactiva. La estrategia proactiva o de previsión de ataques es un conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de seguridad y a desarrollar planes de contingencia. La determinación del daño que un ataque va a provocar en un sistema y las debilidades y puntos vulnerables explotados durante este ataque ayudará a desarrollar la estrategia proactiva.

La estrategia reactiva o estrategia posterior al ataque ayuda al personal de seguridad a evaluar el daño que ha causado el ataque, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia proactiva, a documentar y aprender de la experiencia, y a conseguir que las funciones comerciales se normalicen lo antes posible.

Pruebas

El último elemento de las estrategias de seguridad, las pruebas y el estudio de sus resultados, se lleva a cabo después de que se han puesto en marcha las estrategias reactiva y proactiva. La realización de ataques simulados en sistemas de pruebas o en laboratorios permiten evaluar los lugares en los que hay puntos vulnerables y ajustar las directivas y los controles de seguridad en consecuencia. Estas pruebas no se deben llevar a cabo en los sistemas de producción real, ya que el resultado puede ser desastroso. La carencia de laboratorios y equipos de pruebas a causa de restricciones presupuestarias puede imposibilitar la realización de ataques simulados. Para asegurar los fondos necesarios para las pruebas, es importante que los directivos sean conscientes de los riesgos y consecuencias de los ataques, así como de las medidas de seguridad que se pueden adoptar para proteger al sistema, incluidos los procedimientos de las pruebas. Si es posible, se deben probar físicamente y documentar todos los casos de ataque para determinar las mejores directivas y controles de seguridad posibles que se van a implementar.

Determinados ataques, por ejemplo desastres naturales como inundaciones y rayos, no se pueden probar, aunque una simulación servirá de gran ayuda. Por ejemplo, se puede simular un incendio en la sala de servidores en el que todos los servidores hayan resultado dañados y hayan quedado inutilizables. Este caso puede ser útil para probar la respuesta de los administradores y del personal de seguridad, y para determinar el tiempo que se tardará en volver a poner la organización en funcionamiento.

La realización de pruebas y de ajustes en las directivas y controles de seguridad en función de los resultados de las pruebas es un proceso iterativo. Nunca termina, ya que debe evaluarse y revisarse de forma periódica para poder implementar mejoras.

Equipos de respuesta a incidentes

Es aconsejable formar un equipo de respuesta a incidentes. Este equipo debe estar implicado en los trabajos proactivos del profesional de la seguridad. Entre éstos se incluyen:

TESIS CON
FALLA DE ORIGEN

- El desarrollo de instrucciones para controlar incidentes.
- La identificación de las herramientas de software para responder a incidentes y eventos.
- La investigación y desarrollo de otras herramientas de seguridad informática.
- La realización de actividades formativas y de motivación.
- La realización de investigaciones acerca de virus.
- La ejecución de estudios relativos a ataques al sistema.

Estos trabajos proporcionarán los conocimientos que la organización puede utilizar y la información que hay que distribuir antes y durante los incidentes. Una vez que el administrador de seguridad y el equipo de respuesta a incidentes han realizado estas funciones proactivas, el administrador debe delegar la responsabilidad del control de incidentes al equipo de respuesta a incidentes.

Esto no significa que el administrador no deba seguir implicado o formar parte del equipo, sino que no tenga que estar siempre disponible, necesariamente, y que el equipo debe ser capaz de controlar los incidentes por sí mismo.

El equipo será el responsable de responder a incidentes como virus, gusanos o cualquier otro código dañino; invasión; engaños; desastres naturales y ataques del personal interno. El equipo también debe participar en el análisis de cualquier evento inusual que pueda estar implicado en la seguridad de los equipos o de la red.

TESIS CON
FALLA DE ORIGEN

Metodología para la definición de estrategias de seguridad

El esquema que se observa a la derecha es una estrategia de seguridad informática que se puede utilizar para implementar directivas y controles de seguridad con el objeto de aminorar los posibles ataques y amenazas.

Los métodos se pueden utilizar en todos los tipos de ataques a sistemas, independientemente de que sean intencionados, no intencionados o desastres naturales, y, por consiguiente, se puedan volver a utilizar en distintos casos de ataque.

La metodología se basa en los distintos tipos de amenazas, métodos de ataque y puntos vulnerables explicados en "Amenazas a la seguridad". El diagrama de flujo describe la metodología.

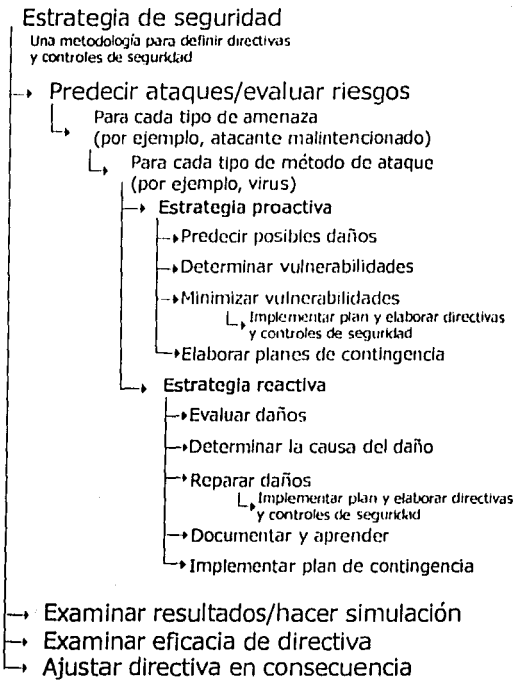


Fig. 2.1 Estrategia de seguridad.[12]

Predecir posibles ataques y analizar riesgos

La primera fase de la metodología esquematizada en el diagrama de flujo es determinar los ataques que se pueden esperar y las formas de defenderse contra ellos. Es imposible estar preparado contra todos los ataques; por lo tanto, hay que prepararse para los que tiene más probabilidad de sufrir la organización. Siempre es mejor prevenir o aminorar los ataques que reparar el daño que han causado.

[12] Metodología propuesta para definir directivas y controles de seguridad (Creación propia)

Para mitigar los ataques es necesario conocer las distintas amenazas que ponen en peligro los sistemas, las técnicas correspondientes que se pueden utilizar para comprometer los controles de seguridad y los puntos vulnerables que existen en las directivas de seguridad. El conocimiento de estos tres elementos de los ataques ayuda a predecir su aparición e, incluso, su duración o ubicación. La predicción de los ataques trata de pronosticar su probabilidad, lo que depende del conocimiento de sus distintos aspectos. Los diferentes aspectos de un ataque se pueden mostrar en la siguiente ecuación:

Amenazas + Motivos + Herramientas y técnicas + Puntos vulnerables = Ataque

Para cada tipo de amenaza se deben considerar todas las amenazas posibles que causan ataques en los sistemas. Entre éstas se incluyen los agresores malintencionados, las amenazas no intencionadas y los desastres naturales. La siguiente ilustración clasifica las distintas amenazas a los sistemas.

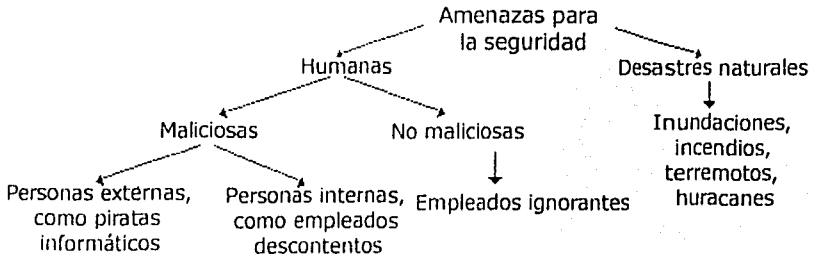


Fig. 2.2 Clasificación de amenasas[13]

Amenazas como empleados ignorantes o descuidados, y los desastres naturales no implican motivos u objetivos; por lo tanto, no se utilizan métodos, herramientas o técnicas predeterminadas para iniciar los ataques. Casi todos estos ataques o infiltraciones en la seguridad se generan internamente; raras veces los va a iniciar alguien ajeno a la organización. Para estos tipos de amenazas, el personal de seguridad necesita implementar estrategias proactivas o reactivas.

Técnicas de Ataque

Para iniciar un ataque, se necesita un método, una herramienta o una técnica para explotar los distintos puntos vulnerables de los sistemas, de las directivas de seguridad y de los controles. Los agresores pueden utilizar varios métodos para iniciar el mismo ataque. Por lo tanto, la estrategia defensiva debe personalizarse para cada tipo de método utilizado en cada tipo de amenaza.

[13] Clasificación de los distintos tipos de amenazas en la seguridad de los sistemas en una organización. (Creación propia)

De nuevo, es importante que los profesionales de la seguridad estén al día en los diferentes métodos, herramientas y técnicas que utilizan los agresores. Puede encontrar una explicación detallada al respecto en "Amenazas a la seguridad".

La siguiente es una lista breve de estas técnicas:

- Ataques de denegación de servicio
- Ataques de invasión
- Ingeniería social
- Virus
- Gusanos
- Caballos de Troya
- Modificación de paquetes
- Repetición de paquetes
- Adivinación de contraseñas
- Interceptación de correo electrónico

Estrategia proactiva

La estrategia proactiva es un conjunto de pasos predefinidos que deben seguirse para evitar ataques antes de que ocurran. Entre estos pasos se incluye observar cómo podría afectar o dañar el sistema, y los puntos vulnerables que explota (pasos 1 y 2). Los conocimientos adquiridos en estas evaluaciones pueden ayudar a implementar las directivas de seguridad que controlarán o aminorarán los ataques. Éstos son los tres pasos de la estrategia proactiva:

1. Determinar el daño que causará el ataque.
2. Establecer los puntos vulnerables y las debilidades que explotará el ataque.
3. Reducir los puntos vulnerables y las debilidades que se ha determinado en el sistema para ese tipo de ataque específico.

El seguimiento de estos pasos para analizar los distintos tipos de ataques tiene una ventaja adicional: comenzará a emerger un modelo, ya que en los diferentes factores se superponen para diferentes ataques. Este modelo puede ser útil al determinar las áreas de vulnerabilidad que plantean el mayor riesgo para la empresa. También es necesario tomar nota del costo que supone la pérdida de los datos frente al de la implementación de controles de seguridad. La ponderación de los riesgos y los costos forma parte de un análisis de riesgos del sistema que se explica en el documento técnico acerca del diseño de la seguridad. Las directivas y controles de seguridad no serán, en ningún caso, totalmente eficaces al eliminar los ataques. Éste es el motivo por el que es necesario desarrollar planes de recuperación y de contingencia en caso de que se quebranten los controles de seguridad.

Determinar el daño posible que puede causar un ataque

Los daños posibles pueden oscilar entre pequeños fallos del equipo y la pérdida, catastrófica, de los datos. El daño causado al sistema dependerá del tipo de ataque. Si es posible, se debe utilizar un entorno de prueba o de laboratorio para clarificar los daños que provocan los diferentes tipos de ataques.

Ello permitirá al personal de seguridad ver el daño físico que causan los ataques experimentales. No todos los ataques causan el mismo daño. Éstos son algunos ejemplos de las pruebas que hay que ejecutar:

- Simular un ataque con virus a través de correo electrónico en el sistema del laboratorio y ver el daño que ha provocado y cómo recuperarse de la situación.
- Utilizar la ingeniería social para adquirir un nombre de usuario y una contraseña de algún empleado ingenuo y observar cómo se comporta.
- Simular lo que ocurriría ante un incendio en la sala de servidores. Mida el tiempo de producción perdido y el tiempo necesario para la recuperación.
- Simular un ataque de virus dañino. Anote el tiempo necesario para recuperar un equipo y multiplique ese tiempo por el número de equipos del sistema infectados para averiguar el tiempo de inactividad y la pérdida de productividad.

También es aconsejable implicar al equipo de respuesta a incidentes ya mencionado, ya que es más probable que un equipo, en lugar de una sola persona, consiga localizar todos los tipos distintos de daños que se han producido.

Seguridad Física

Para considerar la seguridad física es necesario hacerse las siguientes preguntas.

- ¿Hay bloqueos y procedimientos de entrada para obtener acceso a los servidores?
- ¿Es suficiente el aire acondicionado y se limpian regularmente los filtros? ¿Están protegidos los conductos de aire acondicionado contra robos?
- ¿Hay sistemas de alimentación interrumpida, generadores, y se comprueban en los procedimientos de mantenimiento?
- ¿Hay equipo para la extinción de incendios y procedimientos de mantenimiento apropiados para el equipo?
- ¿Hay protección contra el robo de hardware y software? ¿Se guardan los paquetes y licencias de software y las copias de seguridad en lugares seguros?
- ¿Hay procedimientos para almacenar los datos, copias de seguridad y software con licencia en las instalaciones y fuera de ellas?

Seguridad de Datos

Para la seguridad de datos se debe de considerar las siguientes preguntas

- ¿Qué controles de acceso, controles de integridad y procedimientos de copias de seguridad existen para limitar los ataques?
- ¿Hay directivas de privacidad y procedimientos que deban cumplir los usuarios?
- ¿Qué controles de acceso a los datos (autorización, autenticación e implementación) hay?
- ¿Qué responsabilidades tienen los usuarios en la administración de los datos y las aplicaciones?
- ¿Se han definido técnicas de administración de los dispositivos de almacenamiento con acceso directo? ¿Cuál es su efecto en la integridad de los archivos de los usuarios?

Seguridad de red

- ¿Qué tipos de controles de acceso (Internet, conexiones de la red de área extensa, etc.) existen?
- ¿Hay procedimientos de autenticación? ¿Qué protocolos de autenticación se utilizan en las redes de área local, redes de área extensa y servidores de acceso telefónico? ¿Quién tiene la responsabilidad de la administración de la seguridad?
- ¿Qué tipo de medios de red, por ejemplo, cables, conmutadores y enrutadores, se utilizan? ¿Qué tipo de seguridad tienen?
- ¿Se ha implementado la seguridad en los servidores de archivos y de impresoras?
- ¿Hace uso la organización del cifrado y la criptografía en Internet, redes privadas virtuales (VPN), sistemas de correo electrónico y acceso remoto?
- ¿Se ajusta la organización a las normas de redes?

Reducir los puntos vulnerables y debilidades que puede explotar un posible ataque

La reducción de los puntos vulnerables y las debilidades del sistema de seguridad que se determinaron en la evaluación anterior es el primer paso para desarrollar directivas y controles de seguridad eficaces. Ésta es la compensación de la estrategia proactiva. Mediante la reducción de los puntos vulnerables, el personal de seguridad puede hacer disminuir tanto la probabilidad de un ataque como su eficacia, si se produce alguno. Se debe tener cuidado de no implementar controles demasiado estrictos, ya que la disponibilidad de la información se convertiría en un problema. Debe haber un cuidado equilibrio entre los controles de seguridad y el acceso a la información. Los usuarios deben tener la mayor libertad posible para tener acceso a la información.

Elaboración de planes de contingencia

Un plan de contingencia es un plan alternativo que debe desarrollarse en caso de que algún ataque penetre en el sistema y dañe los datos o cualquier otro activo, detenga las operaciones comerciales habituales y reste productividad. El plan se sigue si el sistema no se puede restaurar a tiempo. Su objetivo final es mantener la disponibilidad, integridad y confidencialidad de los datos (es el proverbial "Plan B").

Debe haber un plan para cada tipo de ataque y tipo de amenaza. Cada plan consta de un conjunto de pasos que se han de emprender en el caso de que un ataque logre pasar las directivas de seguridad. El plan de contingencia debe:

- Determinar quién debe hacer qué, en qué momento y en qué lugar para que la organización siga funcionando.
- Ensayarse periódicamente para mantener al personal informado de los pasos de la contingencia actual.
- Abarcar la restauración de las copias de seguridad.
- Explicar la actualización del software antivirus.
- Abarcar el traspaso de la producción a otra ubicación o sitio.

Los siguientes puntos resaltan las distintas tareas que deben evaluarse para desarrollar un plan de contingencia:

- Evaluar las directivas y controles de seguridad de la organización para utilizar todas las oportunidades destinadas a reducir los puntos vulnerables. La evaluación debe tratar el plan y los procedimientos de emergencia actuales de la organización y su integración en el plan de contingencia.
- Evaluar los procedimientos actuales de respuesta ante emergencias y su efecto en el funcionamiento continuo de la organización.
- Desarrollar respuestas planeadas a ataques, integrarlas en el plan de contingencia y anotar hasta qué punto son adecuadas para limitar el daño y reducir el impacto del ataque en las operaciones de procesamiento.
- Evaluar procedimientos de copia de seguridad, que incluyan la documentación más reciente y pruebas de recuperación de desastres, para evaluar su adecuación e integrarlos en el plan de contingencia.
- Evaluar planes de recuperación de desastres para determinar su adecuación con el fin de proporcionar un entorno operativo temporal o a largo plazo. Los planes de recuperación de desastres deben incluir la prueba de los niveles de seguridad necesarios, con el fin de que el personal de seguridad pueda ver si siguen exigiendo la seguridad en todo el proceso de recuperación o en operaciones temporales y el traspaso de la organización otra vez a su sitio de procesamiento original o a un sitio nuevo.

Redactar un documento detallado que describa los distintos descubrimientos en las tareas anteriores. El documento debe mostrar:

- Todos los casos para probar el plan de contingencia.
- El impacto de las dependencias y de la ayuda planeada de fuera de la organización, y las dificultades que la obtención de los recursos esenciales tendrán en el plan.
- Una lista de prioridades observadas en las operaciones de recuperación y el fundamento para establecerlas.

Estrategia reactiva

La estrategia reactiva se implementa cuando ha fallado la estrategia proactiva y define los pasos que deben adoptarse después o durante un ataque. Ayuda a identificar el daño causado y los puntos vulnerables que se explotaron en el ataque, a determinar por qué tuvo lugar, a reparar el daño que causó y a implementar un plan de contingencia, si existe. Tanto la estrategia reactiva como la proactiva funcionan conjuntamente para desarrollar directivas y controles de seguridad con el fin de reducir los ataques y el daño que causan.

El equipo de respuesta a incidentes debe incluirse en los pasos adoptados durante o después del ataque para ayudar a evaluarlo, a documentar el evento y a aprender de él.

Evaluar el daño

Es necesario determinar el daño causado durante el ataque. Esto debe hacerse lo antes posible para que puedan comenzar las operaciones de restauración. Si no se puede evaluar el daño a

tiempo, debe implementarse un plan de contingencia para que puedan proseguir las operaciones comerciales y la productividad normales.

Determinar la causa del daño

Para determinar la causa del daño, es necesario saber a qué recursos iba dirigido el ataque y qué puntos vulnerables se explotaron para obtener acceso o perturbar los servicios. Es necesario revisar los registros del sistema, los registros de auditoría y las pistas de auditoría. Estas revisiones suelen ayudar a descubrir el lugar del sistema en el que se originó el ataque y qué otros recursos resultaron afectados.

Reparar el daño

Es muy importante que el daño se repare lo antes posible para restaurar las operaciones comerciales normales y todos los datos perdidos durante el ataque. Los planes y procedimientos para la recuperación de desastres de la organización (que se tratan en el documento acerca del diseño de la seguridad) deben cubrir la estrategia de restauración. El equipo de respuesta a incidentes también debe poder controlar el proceso de restauración y recuperación, y ayudar en este último.

Documentar y aprender

Es importante documentar el ataque una vez que se ha producido. La documentación debe abarcar todos los aspectos que se conozcan del mismo, entre los que se incluyen el daño que ha causado (en hardware y software, pérdida de datos o pérdida de productividad), los puntos vulnerables y las debilidades que se explotaron durante el ataque, la cantidad de tiempo de producción perdido y los procedimientos tomados para reparar el daño. La documentación ayudará a modificar las estrategias proactivas para evitar ataques futuros o mermar los daños.

Implementar un plan de contingencia

Si ya existe algún plan de contingencia, se puede implementar para ahorrar tiempo y mantener el buen funcionamiento de las operaciones comerciales. Si no hay ningún plan de contingencia, desarrollar un plan apropiado basado de la documentación del paso anterior.

Revisar el resultado y hacer simulaciones

El segundo paso importante en la estrategia de seguridad es revisar los descubrimientos establecidos en el primer paso (predicción del ataque). Tras el ataque o tras defenderse de él, revisar el resultado con respecto al sistema. La revisión debe incluir la pérdida de productividad, la pérdida de datos o de hardware, y el tiempo que se tarda en recuperarlos.

Documentar también el ataque y, si es posible, hacer un seguimiento del lugar en el que se originó, qué métodos se utilizaron para iniciarlo y qué puntos vulnerables se explotaron. Para obtener los mejores resultados posibles, realizar simulaciones en un entorno de prueba.

Revisar la eficacia de las directivas

Si hay directivas para defenderse de un ataque que se ha producido, hay que revisar y comprobar su eficacia. Si no hay directivas, se deben redactar para aminorar o impedir ataques futuros.

Ajustar la directiva en consecuencia

Si la eficacia de la directiva no llega al estándar, hay que ajustarla en consecuencia. Las actualizaciones de las directivas debe realizarlas el personal directivo relevante, los responsables de seguridad, los administradores y el equipo de respuesta a incidentes. Todas las directivas deben seguir las reglas e instrucciones generales de la organización. Por ejemplo, el horario laboral puede ser de 8 a.m. a 6 p.m. Podría existir o crearse una directiva de seguridad que permita a los usuarios conectarse al sistema solamente durante este horario.

Auditoría

Además de planear la seguridad de la información en la base de datos, uno de los objetivos de éste sistema es la auditoría de dicho sistema. Para definir como se planeará las transacciones del sistema es necesario definir el concepto de auditoría de sistemas.

La auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo,de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoría en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad en los sistemas.[14]

Paradigmas Organizacionales en Cuanto a Seguridad

Paradigma: Modelo o ejemplo de algo, En filosofía: Conjunto de ideas filosóficas, teorías científicas y normas metodológicas que influyen en la forma de resolver los problemas en una determinada tradición científica. Sinónimo: prototipo, muestra.

Los paradigmas desempeñan un papel importante en la actual filosofía de la ciencia, a partir de la obra de Thomas S. Kuhn "La estructura de las revoluciones científicas" (1962).

[14] A.J. Thomas I.J. Douglas "Auditoría Informática" Ed. Paraninfo. Segunda Edición Pág. 11

Del paradigma se desprenden las reglas que rigen las investigaciones. Cuando dentro de un paradigma aparecen anomalías excesivas, se produce una revolución científica que consiste precisamente en el cambio de paradigma

Es muy importante que se conozcan los paradigmas que existen en las organizaciones sobre la seguridad, para no encontrarse con un contrincante desconocido.

Entre los principales paradigmas que se pueden encontrar veamos los siguientes:

- Generalmente se tiene la idea que los procedimientos de auditoría es responsabilidad del personal del centro de computo, pero se debe cambiar este paradigma y conocer que estas son responsabilidades del usuario y del departamento de auditoría interna.
- También muchas compañías cuentan con dispositivos de seguridad física para los computadores y se tiene la idea que los sistemas no pueden ser violados si no se ingresa al centro al centro de computo, ya que no se considera el uso terminales y de sistemas remotos.
- Se piensa también que los casos de seguridad que tratan de seguridad de incendio o robo que "eso no me puede suceder a mí" o "es poco probable que suceda".
- También se cree que los computadores y los programas son tan complejos que nadie fuera de su organización los va a entender y no les van a servir, ignorando las personas que puedan captar y usarla para otros fines.
- Los sistemas de seguridad generalmente no consideran la posibilidad de fraude interno que es cometido por el mismo personal en el desarrollo de sus funciones.
- Generalmente se piensa que la seguridad por clave de acceso es inviolable pero no se considera a los delincuentes sofisticados.
- Se suele suponer que los defectos y errores son inevitables.
- También se cree que se hallan fallas porque nada es perfecto.
- Y la creencia que la seguridad se aumenta solo con la inspección.

Por esto se deben analizar estos y otros paradigmas de la organización, también es muy importante que el auditor enfrente y evalúe primero sus propios paradigmas y sus paradigmas académicos.

Planeación de la Auditoría en Informática

Para hacer una adecuada planeación de la auditoría en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de área dentro del organismo a auditar, sus sistemas, organización y equipo.

En el caso de la auditoría en informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de los dos objetivos:[15]

[15] Yann Derrien "Técnicas de la auditoría informática" Ed. Alfaomega marcombo Pág. 35

TESIS CON
FALLA DE ORIGEN

Evaluación de los sistemas y procedimientos.

Para hacer una planeación eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

2.2 Metodología Yourdon

Antes de poder definir un tipo de metodología en particular es necesario conocer aspectos importantes en el entorno de sistemas de información, como son los elementos de un sistema.

Elementos de un Sistema

Una definición básica de sistema es la siguiente: Grupo de elementos interdependientes o que interactúan regularmente formando un todo, a continuación se enumeran diversos ejemplos: un sistema gravitacional, un sistema termodinámico, un sistema de ríos, un sistema telefónico, un sistema de autopistas, el sistema newtoniano de la mecánica, el sistema de mecanografía al tacto, un sistema taxonómico, el sistema decimal, etcétera.

James Grier Miller en su libro Living System destaca 19 subsistemas críticos de todos los sistemas vivientes, haciendo una analogía con los mismos se pueden categorizar de la manera siguiente:

El reproductor, que es capaz de dar origen a otros sistemas similares aquel en el cual se encuentra. En una organización de negocios, pudiera ser una división de planeación de instalaciones que hace nuevas plantas y construye oficinas regionales nuevas.

La frontera, que mantiene unidos a los componentes que conforman el sistema, los protege de tensiones ambientales y excluye o permite la entrada de diversos tipos de materia-energía e información. En una organización de negocios, esto pudiera constituir la planta misma y los guardias u otro personal de seguridad que evitan el ingreso de intrusos indeseables.

- El inyector, que transporta la materia-energía a través de la frontera del sistema desde el medio ambiente. En una organización de negocios, este pudiera ser el departamento de compras o recepción, que introduce la materia prima, los materiales de oficina, etc.
- El distribuidor, que trae material desde el exterior del sistema y lo reparte desde sus subsistemas a cada componente. En una organización de negocios, pudiera estar conformado por las líneas telefónicas, correo electrónico, mensajeros, bandas, etc.
- El convertidor, que cambia ciertos materiales que ingresan al sistema a formas más útiles para los procesos especiales de dicho sistema particular.
- El productor, que forma asociaciones estables durables por períodos significativos con la materia-energía que ingresa al sistema o que egresa de su convertidor. Estos materiales sintetizados pueden servir para crecimiento o reparación de daños o reposición de componentes del sistema.

TESIS CON
FALLA DE ORIGEN

- El subsistema de almacenamiento de materia-energía, que retiene en el sistema, durante diferentes períodos, depósitos de diversos tipos de materia-energía.
- El expulsor, que transmite materia-energía hacia el exterior del sistema en forma de desechos o de productos.
- El motor, que mueve el sistema o a sus partes en relación con todo o parte del medio ambiente, o bien que mueve a los componentes del ambiente.
- El soporte, que mantiene las relaciones espaciales apropiadas entre los componentes del sistema, de manera que pueden interactuar sin ser un lastre o estorbo entre ellos.
- El transductor de entrada, que traen señales portadoras de información al sistema, transformándolas en otras formas de materia-energía adecuadas para su transmisión al interior.
- El transductor interno, que recibe de otros subsistemas o componentes del sistema señales que portan información acerca de alteraciones significativas en dichos subsistemas o componentes, transformándolos en otras formas de materia-energía transmisibles en su interior.
- El canal y la red, que están compuestos por una sola ruta en el espacio físico, o bien por múltiples rutas interconectadas, mediante las cuales las señales portadoras de información se transmiten a todas partes del sistema.
- El decodificador, que altera las claves de información que le es introducida por medio del transductor de entrada o del transductor interno, para dejar una clave privada que pueda ser utilizada internamente por el sistema.
- El asociado, que lleva a cabo la primera etapa del proceso de aprendizaje, formando asociaciones duraderas entre elementos de información dentro del sistema.
- La memoria, que lleva a cabo la segunda etapa del aprendizaje, almacenando diversos tipos de información en el sistema durante diferentes períodos.
- El que decide, que recibe información de los demás subsistemas y les transmite información que sirve para controlar al sistema completo.
- El codificador, que altera la clave de información que se le introduce desde otros subsistemas procesadores de información, convirtiéndola, de una clave privada utilizada internamente por el sistema, en una clave pública que pueden ser interpretada por otros sistemas en su medio ambiente.
- El transductor de salida, que emite señales portadoras de información desde el sistema, transformando los marcadores dentro del sistema en otras formas de materia-energía que pueden ser transmitidas por medio de canales en el medio ambiente del sistema

Sistemas de información más comunes

Existen dos categorías básicas en la clasificación de sistemas:

- Sistemas naturales.
- Sistemas hechos por el hombre.

Es conveniente dividir los sistemas naturales en dos subcategorías básicas:

- Sistemas físicos.
- Sistemas vivientes.

Los sistemas físicos incluyen:

TESIS CON
FALLA DE ORIGEN

- Sistemas estelares: galaxias, sistemas solares, etcétera.
- Sistemas geológicos: ríos, cordilleras, etcétera.
- Sistemas moleculares: organizaciones complejas de átomos.

Los sistemas vivientes comprenden toda gama de animales y plantas que nos rodean, al igual que la raza humana. En lo que respecta a los sistemas hechos por el hombre existen una gran diversidad de sistemas construidos, organizados y mantenidos por humanos, tales como: sistemas sociales, sistemas de transporte, sistemas de comunicación, Sistemas de manufactura, sistemas financieros. En la actualidad, la mayoría de estos sistemas incluyen las computadoras pero es importante señalar que dichos sistemas existían antes de que hubiera computadoras; de hecho, algunos sistemas continúan por completo sin computarizar y podrían permanecer así durante muchas décadas más.

Otros contienen a la computadora como componente, pero también incluyen uno o más componentes no computarizados (o manuales). Los sistemas automatizados son sistemas hechos por el hombre que interactúan con o son controlados por una o más computadoras. Aunque hay diferentes tipos de sistemas automatizados, todos tienden a tener componentes en común:

- El hardware de la computadora: los procesadores, los discos, terminales, impresora, unidades de cinta magnética, etcétera.
- El software de la computadora: Los programas de sistemas tales como sistemas operativos, sistemas de base de datos, programas de control de telecomunicaciones, etcétera.
- Las personas: los que operan el sistema, los que proveen su material de entrada y consumen su material de salida, y los que proveen actividades de procesamiento manual en un sistema.
- Los datos: la información que el sistema recuerda
- Los procedimientos: las políticas formales e instrucciones de operación del sistema.

Una división categórica de los sistemas automatizados es la siguiente:

- Sistemas en línea: es aquel que acepta material de entrada directamente del área donde se creo. También es sistema en el que el material de salida, o resultado de la computación, se devuelve directamente a donde es requerido.
- Sistemas de tiempo real: puede definirse como aquel que controla un ambiente recibiendo datos, procesándolos y devolviéndolos con la suficiente rapidez como para influir en dicho ambiente en ese momento.
- Sistemas de apoyo a decisiones: Estos sistemas computacionales no toman decisiones por si mismos, sino ayudan a los administradores, y a otros profesionistas "trabajadores del conocimiento" de una organización a tomar decisiones inteligentes y documentadas acerca de los diversos aspectos de la operación.
- Sistemas basados en el conocimiento: Estos sistemas contienen grandes cantidades de diversos conocimientos que emplean en el desempeño de una tarea dada. Los sistemas expertos son una especie de sistemas basados en el conocimiento, aunque ambos términos a menudo se utilizan indistintamente.

TESIS CON
FALLA DE ORIGEN

Existen algunos principios generales que son de interés particular para quienes crean sistemas automatizados de información, e incluyen los siguientes:

Entre más especializado sea el sistema, menos capaz es de adaptarse a circunstancias diferentes. Cuanto mayor sea el sistema mayor es el número de sus recursos que deben dedicarse a su mantenimiento diario. Los sistemas siempre forman parte de sistemas mayores y siempre pueden dividirse en sistemas menores y por último, los sistemas crecen.[16]

Análisis Estructurado

Finalidades de un Análisis Estructurado:

- Obtener una descripción lógica del sistema a desarrollar
- Descripción del ámbito del sistema.
- Especificación
  - Funcional
  - De datos
  - De rendimiento
  - De interfez
  - De pruebas

Lo que se persigue con el tipo de análisis estructurado o de "Yourdon" es: Por parte del analista es entender con precisión lo que el usuario quiere, así por parte del usuario es entender con precisión el producto que se le ofrece. Por consiguiente la clave del éxito es una buena comunicación entre el usuario y el analista.[17]

Definición del Análisis Estructurado:

Es la técnica de modelado del flujo, contenido y transformación de la información que influye por un sistema. Nació como complemento al Diseño Estructurado.

La principal característica del diseño estructurado es lo que se denomina como "TOP DOWN" (esto es de arriba hacia abajo)

El diseño es un proceso mediante le cuál se traducen los requisitos en una representación del software.

El diseño es un proceso de resolución de problemas que busca caminos para conseguir los objetivos planeados. Por lo tanto, su meta es crear un sistema que reúna un conjunto de objetivos y esos objetivos son la fuerza que conduce el procesos de diseño.[18]

[16] S.M. Deen "Fundamento de los sistemas de bases de datos", Colección Ciencia Informática 1985. Pág. 43
[17] E. Yourdon, "Análisis Estructurado Moderno" Ed. Prentice Hall, 1994
[18] I. Sommerville, "Software Engineering" Ed. Addison-Wesley 1996 Capítulo 4,5

TESIS CON
FALLA DE ORIGEN

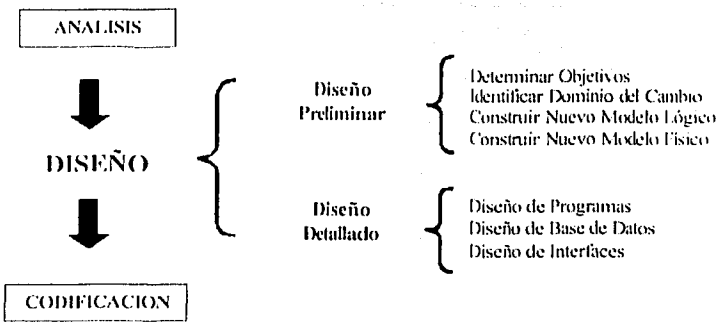


Fig 2.3 Clasificación de las etapas de diseño.[19]

El término de "Análisis Estructurado" fue popularizado por DeMarco a fines de los 70, quien presentó y denominó los símbolos gráficos que permitirían al analista crear modelos de flujo de información. Posteriormente Yourdon, Gane y Sarson y otros presentaron variaciones a la propuesta original. A mediados de los 80 Ward y Mellor proponen ampliaciones para su aplicación en sistemas de tiempo real.

Herramientas usadas el Análisis Estructurado

- Diagrama de Flujo de Datos (DFD)
- Diccionario de Datos
- Especificaciones de Procesos
- Diagramas Entidad-Relación
- Diagramas de Transición de Estados

Diagrama de flujo de Datos

El DFD representa un modelo del flujo de información del sistema y se caracteriza porque:

- Muestra el flujo de la información.
- Muestra las transformaciones aplicadas a los datos desde la entrada hasta la salida
- Especifica QUE hace el sistema.
- Es gráfico
- Es comprensible por los usuarios
- Se puede usar a cualquier nivel de detalle.
- Permite el particionamiento del sistema en diferentes niveles de detalle.

[19] Clasificación de las etapas de diseño, tomada del libro "Software Engineering"

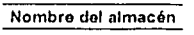
Componentes del diagrama de flujo de datos

Entidades Externas

Con estas entidades externas identifique que algo o alguien envía o recibe información, además marcan los límites del sistema. Notación:

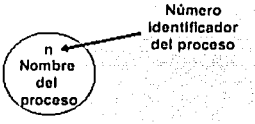
Almacenes de datos

Los almacenes de datos identifican un Depósito (computacional o no) donde se guardan los datos para su posterior uso. Por ejemplo un fichero, una Base de Datos, un archivador. Notación:



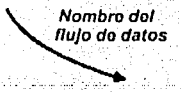
Procesos

Los procesos identifica algo o alguien que transforma y/o manipula flujo de datos. Notación:



Flujos de datos:

Estos representan movimientos de información dentro del sistema y pueden tener 2 o más destinos simultáneos. Notación:



TESIS CON
FALLA DE ORIGEN

La siguiente tabla representa las conexiones permitidas en un DFD.

	Entidades	Procesos	Almacenes
Entidades	X	✓	X
Procesos	✓	✓	✓
Almacenes	X	✓	X

Explosión de un proceso

Consiste en disgregar un proceso padre en un nuevo DFD de mayor detalle. Este se produce a medida que se conocen más actividades internas a dicho proceso. Las normas a seguir al explosionar un proceso son:

- Numeración: Al explosionar el proceso "n", se numerarán los procesos hijos como n1, n2,...
- DFD Balanceado: Todos los flujos que entraban o salían del proceso padre deberán entrar y salir del conjunto de procesos hijos.
- Del DFD obtenido por explosión pueden surgir nuevos flujos correspondientes al tratamiento de errores y excepciones. Asimismo pueden aparecer almacenes de datos privados

Otras normas de construcción de DFDs:

- No debe tenerse en cuenta aspectos de iniciación o terminación de funciones.
- Generalmente, no habrá almacenes de datos en los que solo se escriba.
- Todos los procesos, almacenes de datos, flujos de datos y entidades deben tener asignado un nombre.
- Todos los procesos deben tener al menos un flujo de entrada y otro de salida
- Los DFD deben ser independientes de la implementación.

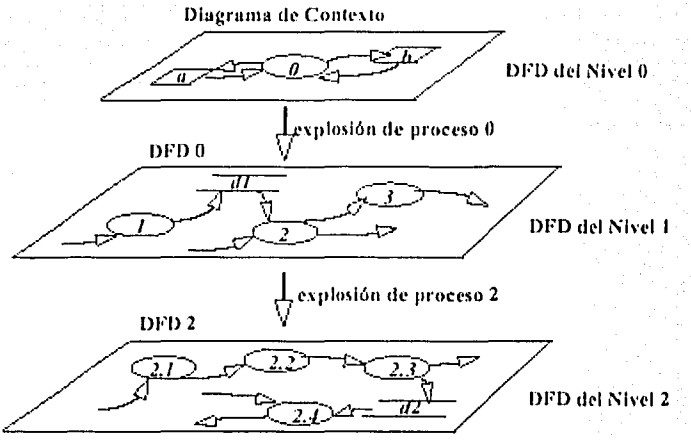


Fig. 2.4 Niveles de un DFD. [20]

Guía para construir un DFD

Para construir un DFD se deben de considerar varios puntos:

- Estudio inicial mediante: entrevistas a usuarios, lecturas de documentos relacionados con el área de estudio
- Identificar: alcance del sistema, información relevante, entidades externa.
- Elaborar el primer borrador del DFD 0, identificando procesos, flujos, almacenes de datos y entidades externas.
- Revisión con el equipo informático. Verificar nombres adecuados en procesos y flujos de datos, verificar que cada proceso y almacén de datos tiene entradas.
- Obtener un segundo borrador de DFD 0 incorporando posibles modificaciones.
- Revisión con el usuario para asegurar que el DFD refleja el sistema. Obtener confirmación por parte del usuario.
- Elaborar DFDs de segundo nivel.
- Confirmar DFD 0 verificándolo con respecto a DFDs de segundo nivel. Verificar que los DFDs están balanceados.
- Revisión final para validar DFD 0 y DFDs de más bajo nivel.

[20] Niveles de un diagrama de flujo de datos

TESIS CON
FALLA DE ORIGEN

Diccionario de Datos

El diccionario de datos contiene la descripción detallada de cada dato del sistema

- Existirá una entrada por cada flujo de datos o almacén de datos que aparezca en los DFDs del sistema.
- Se especificará cada estructura de datos hasta el nivel más elemental

Cada dato debería tener una definición que incluya:

- Comentario que explique el significado en el contexto del sistema
- Comosición, si no es un dato elemental
- Valores posibles, si es un dato elemental

Notación:

= está compuesto de

+ concatenación de datos

( ) dato opcional

{ } repetición

[ ] selección de una de las alternativas

' comentario

@ campo clave para un almacén de datos

| separador de alternativas en el constructor []

Especificación de procesos

Son descripciones de la lógica interna de los procesos de los DFDs de último nivel. Además definen que debe hacerse para transformar las entradas en salidas

Herramientas

- Lenguaje estructurado o pseudocódigo
- Árboles de decisión
- Tablas de decisión
- Diagrama de flujo
- Descripción narrativa

Lenguaje estructurado

Implica utilizar el lenguaje natural con algunas restricciones. Así debe de existir un equilibrio entre la precisión de un lenguaje formal y la informalidad y legibilidad del lenguaje natural. Una sentencia del lenguaje estructurado debería ser

- Una ecuación algebraica, por ejemplo X = (Y*Z)/(Q+14)
- Una sentencia imperativa consiste de un verbo y un objeto
- Combinación de constructores estructurados

Verbos tipo:

Obtener (aceptar o leer) mover borrar

Poner (escribir) reemplazar ordenar

Encontrar(buscar o localizar) calcular validar

Objetos:

- Elementos descritos en el Diccionario de Datos
- Datos locales al proceso
- Constructores estructurados

2.3 Control administrativo en la Seguridad Informática

Como se observo en el punto 2.1 para tener un control administrativo en lo referente a la seguridad informática es necesario llevar acabo los siguientes puntos, que servirán de base para el desarrollo del sistema de control de seguridad en base de datos.

- Evaluar el ambiente del área de computo así como los sistemas que actualmente están operando para tener una visión de la seguridad actual

- Establecer políticas, procedimientos y prácticas del control de datos en la organización

Evaluar el ambiente de seguridad actual

El primer paso en la protección los sistemas es la elaboración de un cálculo de riesgos que permita identificar y priorizar las áreas a proteger. En el proceso de planeación, lo que se hace es reducir las citaciones complejas a lo que parecen ser, (Ackoff) para ello es preciso:

1. Determinar los activos tecnológicos e información de la empresa, y evaluar la importancia que tienen para el desarrollo del negocio. Por ejemplo la información referente a salarios de los empleados debe ser de mayor importancia que la información del inventario de equipo, para una empresa que necesita mantener reservada esa información.

2. Identificar las vulnerabilidades y amenazas, y determinar el nivel de severidad con la que afectan a la seguridad de los activos. Por ejemplo, una vulnerabilidad en un servidor de correo electrónico puede afectar de forma muy directa a la información transmitida a través de e-mail, pero puede no afectar de forma demasiado severa a la seguridad de una base de datos corporativa.
3. Una vez identificados los activos y determinadas las vulnerabilidades que los amenazan, podemos priorizar las áreas que necesitan protección. Por ejemplo, es más urgente proteger una base de datos dedicada a la consulta de saldos por parte de los clientes de un banco cuya importancia no es crítica pero que se encuentra afectado por una vulnerabilidad comúnmente conocida, antes que proteger una base de datos corporativa de carácter confidencial y que no se encuentra afectada de forma directa por ninguna vulnerabilidad.

Para hacer estas actividades es preciso hacer una investigación preliminar y algunas entrevistas previas, con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

Investigación preliminar

Se deberá observar el estado general del área en la cual se implantará el sistema de control de seguridad en base de datos, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización.
Se debe hacer la investigación preliminar solicitando y revisando la información de cada una de las áreas basándose en los siguientes puntos:

Administración.- Se recopila la información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitud de documentos para poder definir el objetivo y alcances del departamento.

Para analizar y dimensionar la estructura por auditar se debe solicitar: A nivel del área de informática.- Objetivos a corto y largo plazo.

Recursos materiales y técnicos.- Solicitar documentos sobre los equipos, número de ellos, localización y características.

- Estudios de viabilidad.
- Número de equipos, localización y las características (de los equipos instalados y por instalar y programados)
- Fechas de instalación de los equipos y planes de instalación.
- Contratos vigentes de compra, renta y servicio de mantenimiento.
- Contratos de seguros.
- Convenios que se tienen con otras instalaciones.
- Configuración de los equipos y capacidades actuales y máximas.
- Planes de expansión.
- Ubicación general de los equipos.
- Políticas de operación.
- Políticas de uso de los equipos.

Sistemas.- Descripción general de los sistemas instalados y de los que estén por instalarse que contengan volúmenes de información.

- Manual de formas.
- Manual de procedimientos de los sistemas.
- Descripción genérica.
- Diagramas de entrada, archivos, salida.
- Salidas.
- Fecha de instalación de los sistemas.
- Proyecto de instalación de nuevos sistemas.

En el momento de hacer la planeación de la auditoría o bien su realización, debemos evaluar que pueden presentarse las siguientes situaciones.

Se solicita la información y se ve que:

- No tiene y se necesita.
- No se tiene y no se necesita.

Se tiene la información pero:

- No se usa.
- Es incompleta.
- No esta actualizada.
- No es la adecuada.
- Se usa, está actualizada, es la adecuada y está completa.

En el caso de No se tiene y no se necesita, se debe evaluar la causa por la que no es necesaria. En el caso de No se tiene pero es necesaria, se debe recomendar que se elabore de acuerdo con las necesidades y con el uso que se le va a dar. En el caso de que se tenga la información pero no se utilice, se debe analizar por que no se usa. En caso de que se tenga la información, se debe analizar si se usa, si está actualizada, si es la adecuada y si está completa.
El éxito del análisis crítico depende de las consideraciones siguientes:

- Estudiar hechos y no opiniones (no se toman en cuenta los rumores ni la información sin fundamento)
- Investigar las causas, no los efectos.
- Atender razones, no excusas.
- No confiar en la memoria, preguntar constantemente.
- Criticar objetivamente y a fondo todos los informes y los datos recabados.

Personal Participante

Una de las partes más importantes dentro de la planeación de la auditoría en informática es el personal que deberá participar y sus características. Uno de los esquemas generalmente aceptados para tener un adecuado control es que el personal que intervengan esté debidamente capacitado, con alto sentido de moralidad, al cual se le exija la optimización de recursos (eficiencia) y se le retribuya o compense justamente por su trabajo.

Con estas bases se debe considerar las características de conocimientos, práctica profesional y capacitación que debe tener el personal que intervendrá en la auditoría. En primer lugar se debe

pensar que hay personal asignado por la organización, con el suficiente nivel para poder coordinar el desarrollo de la auditoría, proporcionar toda la información que se solicite y programar las reuniones y entrevistas requeridas.

Éste es un punto muy importante ya que, de no tener el apoyo de la alta dirección, ni contar con un grupo multidisciplinario en el cual estén presentes una o varias personas del área a auditar, sería casi imposible obtener información en el momento y con las características deseadas.

También se debe contar con personas asignadas por los usuarios para que en el momento que se solicite información o bien se efectúe alguna entrevista de comprobación de hipótesis, nos proporcionen aquello que se esta solicitando, y complementen el grupo multidisciplinario, ya que se debe analizar no sólo el punto de vista de la dirección de informática, sino también el del usuario del sistema.

Para completar el grupo, como colaboradores directos en la realización de la auditoría se deben tener personas con las siguientes características:

- Técnico en informática.
- Experiencia en el área de informática.
- Experiencia en operación y análisis de sistemas.
- Conocimientos de los sistemas más importantes.

En caso de sistemas complejos se deberá contar con personal con conocimientos y experiencia en áreas específicas como base de datos, redes, etc.

Lo anterior no significa que una sola persona tenga los conocimientos y experiencias señaladas, pero si deben intervenir una o varias personas con las características apuntadas.

Evaluación de sistemas

Para poder implantar el sistema de control de seguridad en base de datos en necesario también hacer una evaluación de los sistemas que operan y están por operar el la organización, así como la forma en que se implementan y trabajan.

La elaboración de sistemas debe ser evaluada con mucho detalle, para lo cual se debe revisar si existen realmente sistemas entrelazados como un todo o bien si existen programas aislados. Otro de los factores a evaluar es si existe un plan estratégico para la elaboración de los sistemas o si se están elaborados sin el adecuado señalamiento de prioridades y de objetivos. El plan estratégico deberá establecer los servicios que se presentarán en un futuro contestando preguntas como las siguientes:

- ¿Cuáles servicios se implementarán?
- ¿Cuándo se pondrán a disposición de los usuarios?
- ¿Qué características tendrán?
- ¿Cuántos recursos se requerirán?

La estrategia de desarrollo deberá establecer las nuevas aplicaciones, recursos y la arquitectura en que estarán fundamentados:

- ¿Qué aplicaciones serán desarrolladas y cuando?
- ·¿Qué tipo de archivos se utilizarán y cuando?
- ·¿Qué bases de datos serán utilizarán y cuando?
- ·¿Qué lenguajes se utilizarán y en que software?
- ·¿Qué tecnología será utilizada y cuando se implementará?
- ·¿Cuantos recursos se requerirán aproximadamente?
- ·¿Cuál es aproximadamente el monto de la inversión en hardware y software?

En lo referente a la consulta a los usuarios, el plan estratégico debe definir los requerimientos de información de la dependencia.

- ¿Qué estudios van a ser realizados al respecto?
- ·¿Qué metodología se utilizará para dichos estudios?
- ·¿Quién administrará y realizará dichos estudios?

En el área de auditoría interna debe evaluarse cuál ha sido la participación del auditor y los controles establecidos.

Por último, el plan estratégico determina la planeación de los recursos.

- ·¿Contempla el plan estratégico las ventajas de la nueva tecnología?
- ·¿Cuál es la inversión requerida en servicios, desarrollo y consulta a los usuarios?

El proceso de planeación de sistemas deberá asegurarse de que todos los recursos requeridos estén claramente identificados en el plan de desarrollo de aplicaciones y datos. Estos recursos (hardware, software y comunicaciones) deberán ser compatibles con la arquitectura y la tecnología, conque se cuenta actualmente.

Los sistemas deben evaluarse de acuerdo con el ciclo de vida que normalmente siguen: requerimientos del usuario, estudio de factibilidad, diseño general, análisis, diseño lógico, desarrollo físico, pruebas, implementación, evaluación, modificaciones, instalación, mejoras. Y se vuelve nuevamente al ciclo inicial, el cual a su vez debe comenzar con el de factibilidad.

La primera etapa a evaluar del sistema es el estudio de factibilidad, el cual debe analizar si el sistema es factible de realizarse, cuál es su relación costo/beneficio y si es recomendable elaborarlo.

Se deberá solicitar el estudio de factibilidad de los diferentes sistemas que se encuentren en operación, así como los que estén en la fase de análisis para evaluar si se considera la disponibilidad y características del equipo, los sistemas operativos y lenguajes disponibles, la necesidad de los usuarios, las formas de utilización de los sistemas, el costo y los beneficios que reportará el sistema, el efecto que producirá en quienes lo usarán y el efecto que éstos tendrán sobre el sistema y la congruencia de los diferentes sistemas.

En el caso de sistemas que estén funcionando, se deberá comprobar si existe el estudio de factibilidad con los puntos señalados y compararse con la realidad con lo especificado en el estudio de factibilidad.

Por ejemplo en un sistema que el estudio de factibilidad señaló determinado costo y una serie de beneficios de acuerdo con las necesidades del usuario, debemos comparar cual fue su costo real y evaluar si se satisficieron las necesidades indicadas como beneficios del sistema.

Para investigar el costo de un sistema se debe considerar, con una exactitud razonable, el costo de los programas, el uso de los equipos (compilaciones, programas, pruebas, paralelos), tiempo, personal y operación, cosa que en la práctica son costos directos, indirectos y de operación.

Los beneficios que justifiquen el desarrollo de un sistema pueden ser el ahorro en los costos de operación, la reducción del tiempo de proceso de un sistema. Mayor exactitud, mejor servicio, una mejoría en los procedimientos de control, mayor confiabilidad y seguridad.

Control de datos

Los datos son uno de los recursos más valiosos de las organizaciones y, aunque son intangibles, necesitan ser controlados y auditados con el mismo cuidado que los demás inventarios de la organización, por lo cual se debe tener presente:

a) La responsabilidad de los datos es compartida conjuntamente por alguna función determinada y el departamento de cómputo.
b) Un problema de dependencia que se debe considerar es el que se origina por la duplicidad de los datos y consiste en poder determinar los propietarios o usuarios posibles(principalmente en el caso de redes y banco de datos) y la responsabilidad de su actualización y consistencia.
c) Los datos deberán tener una clasificación estándar y un mecanismo de identificación que permita detectar duplicidad y redundancia dentro de una aplicación y de todas las aplicaciones en general.
d) Se deben relacionar los elementos de los datos con las bases de datos donde están almacenados, así como los reportes y grupos de procesos donde son generados.

Control de los datos fuente y manejo de cifras de control

La mayoría de los Delitos por computadora son cometidos por modificaciones de datos fuente al:

- Suprimir u omitir datos.
- Adicionar Datos.
- Alterar datos.
- Duplicar procesos.

Esto es de suma importancia en caso de equipos de cómputo que cuentan con sistemas en línea, en los que los usuarios son los responsables de la captura y modificación de la información al tener un adecuado control con señalamiento de responsables de los datos(uno de los usuarios debe ser el único responsable de determinado dato), con claves de acceso de acuerdo a niveles.

El primer nivel es el que puede hacer únicamente consultas. El segundo nivel es aquel que puede hacer captura, modificaciones y consultas y el tercer nivel es el que solo puede hacer todos lo anterior y además puede realizar bajas.

Lo primero que se debe evaluar es la entrada de la información y que se tengan las cifras de control necesarias para determinar la veracidad de la información.

Control de Operación

La eficiencia y el costo de la operación de un sistema de cómputo se ven fuertemente afectados por la calidad e integridad de la documentación requerida para el proceso en la computadora. El objetivo del presente ejemplo de cuestionario es señalar los procedimientos e instructivos formales de operación, analizar su estandarización y evaluar el cumplimiento de los mismos.

1. ¿Existen procedimientos formales para la operación del sistema de computo?
2. ¿Están actualizados los procedimientos?
3. Indique la periodicidad de la actualización de los procedimientos:
4. Indique el contenido de los instructivos de operación para cada aplicación:
5. ¿Existen órdenes de proceso para cada corrida en la computadora (incluyendo pruebas, compilaciones y producción)?
6. ¿Son suficientemente claras para los operadores estas órdenes?
7. ¿Existe una estandarización de las ordenes de proceso?
8. ¿Existe un control que asegure la justificación de los procesos en el computador? (Que los procesos que se están autorizados y tengan una razón de ser procesados.
9. ¿Cómo programan los operadores los trabajos dentro del departamento de cómputo?
10. ¿Los retrasos o incumplimiento con el programa de operación diaria, se revisa y analiza?
11. ¿Quién revisa este reporte en su caso?
12. Analice la eficiencia con que se ejecutan los trabajos dentro del departamento de cómputo, tomando en cuenta equipo y operador, a través de inspección visual, y describa sus observaciones.
13. ¿Existen procedimientos escritos para la recuperación del sistema en caso de falla?
14. ¿Cómo se actúa en caso de errores?
15. ¿Existen instrucciones especificas para cada proceso, con las indicaciones pertinentes?
16. ¿Se tienen procedimientos específicos que indiquen al operador que hacer cuando un programa interrumpe su ejecución u otras dificultades en proceso?
17. ¿Puede el operador modificar los datos de entrada?
18. ¿Se prohíbe a analistas y programadores la operación del sistema que programo o analizo?
19. ¿Se prohíbe al operador modificar información de archivos o bibliotecas de programas?
20. ¿El operador realiza funciones de mantenimiento diario en dispositivos que así lo requieran?
21. ¿Las intervenciones de los operadores:
    se limitan los mensajes esenciales? SI ( ) NO ( )
22. ¿Se tiene un control adecuado sobre los sistemas y programas que están en operación?
23. ¿Cómo controlan los trabajos dentro del departamento de cómputo?
24. ¿Se rota al personal de control de información con los operadores procurando un entrenamiento cruzado y evitando la manipulación fraudulenta de datos?
25. ¿Cuentan los operadores con una bitácora para mantener registros de cualquier evento y acción tomada por ellos?

26. Verificar que exista un registro de funcionamiento que muestre el tiempo de paros y mantenimiento o instalaciones de software.
27.¿Existen procedimientos para evitar las corridas de programas no autorizados?
28. ¿Existe un plan definido para el cambio de turno de operaciones que evite el descontrol y discontinuidad de la operación.
29. Verificar que sea razonable el plan para coordinar el cambio de turno.
30. ¿Se hacen inspecciones periódicas de muestreo?
31. Enuncie los procedimientos mencionados en el inciso anterior:
32. ¿Se permite a los operadores el acceso a los diagramas de flujo, programas fuente, etc. fuera del departamento de cómputo?
33. ¿Se controla estrictamente el acceso a la documentación de programas o de aplicaciones rutinarias?
34. Verifique que los privilegios del operador se restrinjan a aquellos que le son asignados a la clasificación de seguridad de operador.
35. ¿Existen procedimientos formales que se deban observar antes de que sean aceptados en operación, sistemas nuevos o modificaciones a los mismos?
36. ¿Estos procedimientos incluyen corridas en paralelo de los sistemas modificados con las versiones anteriores?
37. ¿Durante cuanto tiempo?
38. ¿Que precauciones se toman durante el periodo de implantación?
39. ¿Quién da la aprobación formal cuando las corridas de prueba de un sistema modificado o nuevo están acordes con los instructivos de operación.
40. ¿Se catalogan los programas liberados para producción rutinaria?
41. Mencione que instructivos se proporcionan a las personas que intervienen en la operación rutinaria de un sistema.
42. Indique que tipo de controles tiene sobre los archivos magnéticos de los archivos de datos, que aseguren la utilización de los datos precisos en los procesos correspondientes.
43. ¿Existe un lugar para archivar las bitácoras del sistema del equipo de cómputo?
44. Indique como está organizado este archivo de bitácora.
45. ¿Cuál es la utilización sistemática de las bitácoras?
46. ¿Además de las mencionadas anteriormente, que otras funciones o áreas se encuentran en el departamento de cómputo actualmente?
47. Verifique que se lleve un registro de utilización del equipo diario, sistemas en línea y batch, de tal manera que se pueda medir la eficiencia del uso de equipo.
48. ¿Se tiene inventario actualizado de los equipos y terminales con su localización?
49. ¿Cómo se controlan los procesos en línea?
50. ¿Se tienen seguros sobre todos los equipos?
51. ¿Conque compañía?
Solicitar pólizas de seguros y verificar tipo de seguro y montos.
52. ¿Cómo se controlan las llaves de acceso (Password)?.

Controles de Salida

1. ¿Se tienen copias de los archivos en otros locales?
2. ¿Dónde se encuentran esos locales?
3. ¿Que seguridad física se tiene en esos locales?
4. ¿Que confidencialidad se tiene en esos locales?
5. ¿Quién entrega los documentos de salida?
6. ¿En que forma se entregan?
7. ¿Que documentos?
8. ¿Que controles se tienen?
9. ¿Se tiene un responsable (usuario) de la información de cada sistema? ¿Cómo se atienden solicitudes de información a otros usuarios del mismo sistema?
10. ¿Se destruye la información utilizada, o bien que se hace con ella?

Control de Medios de Almacenamiento Masivo

Los dispositivos de almacenamiento representan, para cualquier centro de cómputo, archivos extremadamente importantes cuya pérdida parcial o total podría tener repercusiones muy serias, no sólo en la unidad de informática, sino en la dependencia de la cual se presta servicio. Una dirección de informática bien administrada debe tener perfectamente protegidos estos dispositivos de almacenamiento, además de mantener registros sistemáticos de la utilización de estos archivos, de modo que servirán de base a registros sistemáticos de la utilización de estos archivos, de modo que sirvan de base a los programas de limpieza (borrado de información), principalmente en el caso de las cintas.

Además se deben tener perfectamente identificados los carretes para reducir la posibilidad de utilización errónea o destrucción de la información. Un manejo adecuado de estos dispositivos permitirá una operación más eficiente y segura, mejorando además los tiempos de procesos.

Control de almacenamiento masivo

Objeticos:
El objetivo de este cuestionario es evaluar la forma como se administran los dispositivos de almacenamiento básico de la dirección.

1. Los locales asignados a la cintoteca y discoteca tienen:
   - Aire acondicionado ( )
   - Protección contra el fuego ( )
   - Cerradura especial ( )
   - Otra
2. ¿Tienen la cintoteca y discoteca protección automática contra el fuego?
3. ¿Que información mínima contiene el inventario de la cintoteca y la discoteca?
   Número o clave del usuario ( )
   Número del archivo lógico ( )
   Nombre del sistema que lo genera ( )
   Fecha de expiración del archivo ( )
   Fecha de expiración del archivo ( )

Número de volumen ( )
Otros

4. ¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos?
5. En caso de existir discrepancia entre las cintas o discos y su contenido, se resuelven y explican satisfactoriamente las discrepancias?
6. ¿Que tan frecuentes son estas discrepancias?
7. ¿Se tienen procedimientos que permitan la reconstrucción de un archivo en cinta a disco, el cual fue inadvertidamente destruido?
8. ¿Se tienen identificados los archivos con información confidencial y se cuenta con claves de acceso?
9. ¿Existe un control estricto de las copias de estos archivos?
10. ¿Que medio se utiliza para almacenarlos?
11. ¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?
12. ¿Se certifica la destrucción o baja de los archivos defectuosos?
13. ¿Se registran como parte del inventario las nuevas cintas que recibe la biblioteca?
14 ¿Se tiene un responsable, por turno, de la cintoteca y discoteca?
15. ¿Se realizan auditorías periódicas a los medios de almacenamiento?
16. ¿Que medidas se toman en el caso de extravío de algún dispositivo de almacenamiento?
18. ¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado?
19. ¿Se tiene relación del personal autorizado para firmar la salida de archivos confidenciales?
20. ¿Existe un procedimiento para registrar los archivos que se prestan y la fecha en que se devolverán?
21. ¿Se lleva control sobre los archivos prestados por la instalación?
22. En caso de préstamo ¿Conque información se documentan?

Nombre de la institución a quién se hace el préstamo.

- echa de recepción ( )
- fecha en que se debe devolver ( )
- archivos que contiene ( )
- formatos ( )
- cifras de control ( )
- código de grabación ( )
- nombre del responsable que los presto ( )
- otros

23. Indique qué procedimiento se sigue en el reemplazo de las cintas que contienen los archivos maestros:
24. ¿Se conserva la cinta maestra anterior hasta después de la nueva cinta?
25. ¿El cintotecario controla la cinta maestra anterior previendo su uso incorrecto o su eliminación prematura?
26. ¿La operación de reemplazo es controlada por el cintotecario?
27. ¿Se utiliza la política de conservación de archivos hijo-padre-abuelo?
28. En los procesos que manejan archivos en línea, ¿Existen procedimientos para recuperar los archivos?
29. ¿Estos procedimientos los conocen los operadores?
30. ¿Con que periodicidad se revisan estos procedimientos?
31. ¿Existe un responsable en caso de falla?
32. ¿Explique que políticas se siguen para la obtención de archivos de respaldo?

33. ¿Existe un procedimiento para el manejo de la información de la cintoteca?
34. ¿Lo conoce y lo sigue el cintotecario?
35. ¿Se distribuyen en forma periódica entre los jefes de sistemas y programación informes de archivos para que liberen los dispositivos de almacenamiento?

Control de Mantenimiento

Como se sabe existen básicamente tres tipos de contrato de mantenimiento: El contrato de mantenimiento total que incluye el mantenimiento correctivo y preventivo, el cual a su vez puede dividirse en aquel que incluye las partes dentro del contrato y el que no incluye partes. El contrato que incluye refacciones es propiamente como un seguro, ya que en caso de descompostura el proveedor debe proporcionar las partes sin costo alguno. Este tipo de contrato es normalmente mas caro, pero se deja al proveedor la responsabilidad total del mantenimiento a excepción de daños por negligencia en la utilización del equipo. (Este tipo de mantenimiento normalmente se emplea en equipos grandes).

El segundo tipo de mantenimiento es "por llamada", en el cual en caso de descompostura se le llama al proveedor y éste cobra de acuerdo a una tarifa y al tiempo que se requiera para componerlo(casi todos los proveedores incluyen, en la cotización de compostura, el tiempo de traslado de su oficina a donde se encuentre el equipo y viceversa). Este tipo de mantenimiento no incluye refacciones.

El tercer tipo de mantenimiento es el que se conoce como "en banco", y es aquel en el cual el cliente lleva a las oficinas del proveedor el equipo, y este hace una cotización de acuerdo con el tiempo necesario para su compostura mas las refacciones (este tipo de mantenimiento puede ser el adecuado para computadoras personales).

Al evaluar el mantenimiento se debe primero analizar cual de los tres tipos es el que más nos conviene y en segundo lugar pedir los contratos y revisar con detalles que las cláusulas estén perfectamente definidas en las cuales se elimine toda la subjetividad y con penalización en caso de incumplimiento, para evitar contratos que sean parciales.

Para poder exigirle el cumplimiento del contrato de debe tener un estricto control sobre las fallas, frecuencia, y el tiempo de reparación. Para evaluar el control que se tiene sobre el mantenimiento y las fallas se pueden utilizar los siguientes cuestionarios:
1. Especifique el tipo de contrato de mantenimiento que se tiene (solicitar copia del contrato).
2. ¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de computo?
3. ¿Se lleva a cabo tal programa?
4. ¿Existen tiempos de respuesta y de compostura estipulados en los contratos?
5. Si los tiempos de reparación son superiores a los estipulados en el contrato, ¿Qué acciones correctivas se toman para ajustarlos a lo convenido?
6. Solicite el plan de mantenimiento preventivo que debe ser proporcionado por el proveedor.-
7. ¿Cómo se notifican las fallas?
8. ¿Cómo se les da seguimiento?

Orden en el Centro de Cómputo

Una dirección de Sistemas de Información bien administrada debe tener y observar reglas relativas al orden y cuidado del departamento de cómputo. Los dispositivos del sistema de cómputo, los archivos magnéticos, pueden ser dañados si se manejan en forma inadecuada y eso puede traducirse en perdidas irreparables de información o en costos muy elevados en la reconstrucción de archivos. Se deben revisar las disposiciones y reglamentos que coadyuven al mantenimiento del orden dentro del departamento de cómputo.

Seguridad lógica y confidencial

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También puede ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional.

Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos. Antes esta situación, en el transcurso del siglo XX, el mundo ha sido testigo de la transformación de algunos aspectos de seguridad y de derecho.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar el llamado ""virus" de las computadoras, el cual aunque tiene diferentes intenciones se encuentra principalmente para paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco.

Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus.
El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de las computadoras grandes, y los principales proveedores ponen a disposición de clientes algunos de estos paquetes.

El sistema integral de seguridad debe comprender:

- Elementos administrativos
- Definición de una política de seguridad
- Organización y división de responsabilidades
- Seguridad física y contra catástrofes(incendio, terremotos, etc.)
- Prácticas de seguridad del personal
- Elementos técnicos y procedimientos

- Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.
- Aplicación de los sistemas de seguridad, incluyendo datos y archivos
- El papel de los auditores, tanto internos como externos
- Planeación de programas de desastre y su prueba.

Se debe evaluar el nivel de riesgo que puede tener la información para poder hacer un adecuado estudio costo/beneficio entre el costo por perdida de información y el costo de un sistema de seguridad, para lo cual se debe considerar lo siguiente:

- Clasificar la instalación en términos de riesgo (alto, mediano, pequeño).
- Identificar aquellas aplicaciones que tengan un alto riesgo.
- Cuantificar el impacto en el caso de suspensión del servicio en aquellas aplicaciones con un alto riesgo.
- Formular las medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera.
- La justificación del costo de implantar las medidas de seguridad para poder clasificar el riesgo e identificar las aplicaciones de alto Riesgo, se debe preguntar lo siguiente:
  - Que sucedería si no se puede usar el sistema?
  - Si la contestación es que no se podría seguir trabajando, esto nos sitúa en un sistema de alto riego.
- La siguiente pregunta es:
  - ¿Que implicaciones tiene el que no se obtenga el sistema y cuanto tiempo podríamos estar sin utilizarlo?
  - ¿Existe un procedimiento alterno y que problemas nos ocasionaría?
  - ¿Que se ha hecho para un caso de emergencia?

Una vez que se ha definido, el grado de riesgo, hay que elaborar una lista de los sistemas con las medias preventivas que se deben tomar, así como las correctivas en caso de desastre señalándole a cada uno su prioridad.
Hay que tener mucho cuidado con la información que sale de la oficina, su utilización y que sea borrada al momento de dejar la instalación que está dando respaldo.

Para clasificar la instalación en términos de riesgo se debe:

- Clasificar los datos, información y programas que contienen información confidencial que tenga un alto valor dentro del mercado de competencia de una organización, e información que sea de difícil recuperación.
- Identificar aquella información que tenga un gran costo financiero en caso de pérdida o bien puede provocar un gran impacto en la toma de decisiones.
- Determinar la información que tenga una gran pérdida en la organización y, consecuentemente, puedan provocar hasta la posibilidad de que no pueda sobrevivir sin esa información.

Para cuantificar el riesgo es necesario que se efectúen entrevistas con los altos niveles administrativos que sean directamente afectados por la suspensión en el procesamiento y que cuantifiquen el impacto que les puede causar este tipo de situaciones.

Para evaluar las medidas de seguridad se debe:

- Especificar la aplicación, los programas y archivos.
- Las medidas en caso de desastre, pérdida total, abuso y los planes necesarios.
- Las prioridades que se deben tomar en cuanto a las acciones a corto y largo plazo.
- En cuanto a la división del trabajo se debe evaluar que se tomen las siguientes precauciones, las cuales dependerán del riesgo que tenga la información y del tipo y tamaño de la organización.
- El personal que prepara la información no debe tener acceso a la operación.
- Los análisis y programadores no deben tener acceso al área de operaciones y viceversa.
- Los operadores no debe tener acceso restringido a las librerías ni a los lugares donde se tengan los archivos almacenados; es importante separar las funciones de librería y de operación.
- Los operadores no deben ser los únicos que tengan el control sobre los trabajos procesados y no deben hacer las correcciones a los errores detectados.

Al implantar sistemas de seguridad puede, reducirse la flexibilidad en el trabajo, pero no debe reducir la eficiencia.

Seguridad Física

El objetivo es establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de datos, información debido a contingencias como incendio, inundaciones, huelgas, disturbios, sabotaje, etc. y continuar en medio de emergencia hasta que sea restaurado el servicio completo.
Entre las precauciones que se deben revisar están:

- Los conductos del aire acondicionado deben estar limpios, ya que son una de las principales causas del polvo y se habrá de contar con detectores de humo que indiquen la posible presencia de fuego.
- En las instalaciones de alto riesgo se debe tener equipo de fuente no interrumpible, tanto en la computadora como en la red y los equipos de teleproceso.
- En cuanto a los extintores, se debe revisar en número de estos, su capacidad, fácil acceso, peso y tipo de producto que utilizan. Es muy frecuente que se tengan los extintores, pero puede suceder que no se encuentren recargados o bien que sean de difícil acceso de un peso tal que sea difícil utilizarlos.
- Esto es común en lugares donde se encuentran trabajando hombres y mujeres y los extintores están a tal altura o con un peso tan grande que una mujer no puede utilizarlos.
- Otro de los problemas es la utilización de extintores inadecuados que pueden provocar mayor perjuicio a las máquinas (extintores líquidos) o que producen gases tóxicos.
- También se debe ver si el personal sabe usar los equipos contra incendio y si ha habido prácticas en cuanto a su uso.
- Se debe verificar que existan suficientes salidas de emergencia y que estén debidamente controladas para evitar robos por medio de estas salidas.
- Los materiales mas peligrosos son las cintas magnéticas que al quemarse, producen gases tóxicos y el papel carbón que es altamente inflamable.

Seguridad en la utilización de equipo

En la actualidad los programas y los equipos son altamente sofisticados y sólo algunas personas dentro del centro de cómputo conocen al detalle el diseño, lo que puede provocar que puedan producir algún deterioro a los sistemas si no se toman las siguientes medidas:

1) Se debe restringir el acceso a los programas y a los archivos.
2) Los operadores deben trabajar con poca supervisión y sin la participación de los programadores, y no deben modificar los programas ni los archivos.
3) Se debe asegurar en todo momento que los datos y archivos usados sean los adecuados, procurando no usar respaldos inadecuados.
4) No debe permitirse la entrada a la red a personas no autorizadas, ni a usar las terminales.
5) Se deben realizar periódicamente una verificación física del uso de terminales y de los reportes obtenidos.
6) Se deben monitorear periódicamente el uso que se le está dando a las terminales.
7) Se deben hacer auditorías periódicas sobre el área de operación y la utilización de las terminales.
8) El usuario es el responsable de los datos, por lo que debe asegurarse que los datos recolectados sean procesados completamente. Esto sólo se logrará por medio de los controles adecuados, los cuales deben ser definidos desde el momento del diseño general del sistema.
9) Deben existir registros que reflejen la transformación entre las diferentes funciones de un sistema.
10) Debe controlarse la distribución de las salidas (reportes, cintas, etc.).
11) Se debe guardar copias de los archivos y programas en lugares ajenos al centro de cómputo y en las instalaciones de alta seguridad; por ejemplo: los bancos.
12) Se debe tener un estricto control sobre el acceso físico a los archivos.
13) En el caso de programas, se debe asignar a cada uno de ellos, una clave que identifique el sistema, subsistema, programa y versión.

También evitará que el programador ponga nombres que nos signifiquen nada y que sean difíciles de identificar, lo que evitará que el programador utilice la computadora para trabajos personales. Otro de los puntos en los que hay que tener seguridad es en el manejo de información. Para controlar este tipo de información se debe:
1) Cuidar que no se obtengan fotocopias de información confidencial sin la debida autorización.
2) Sólo el personal autorizado debe tener acceso a la información confidencial.
3) Controlar los listados tanto de los procesos correctos como aquellos procesos con terminación incorrecta.
4) Controlar el número de copias y la destrucción de la información y del papel carbón de los reportes muy confidenciales.
El factor más importante de la eliminación de riesgos en la programación es que todos los programas y archivos estén debidamente documentados.

El siguiente factor en importancia es contar con los respaldos, y duplicados de los sistemas, programas, archivos y documentación necesarios para que pueda funcionar el plan de emergencia.

- Equipo, programas y archivos
- Control de aplicaciones por terminal
- Definir una estrategia de seguridad de la red y de respaldos
- Requerimientos físicos.
- Estándar de archivos.
- Auditoría interna en el momento del diseño del sistema, su implantación y puntos de verificación y control.

Seguridad al restaurar el equipo

En un mundo que depende cada día mas de los servicios proporcionados por las computadoras, es vital definir procedimientos en caso de una posible falta o siniestro. Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño causado, lo que permitirá recuperar en el menor tiempo posible el proceso perdido. También se debe analizar el impacto futuro en el funcionamiento de la organización y prevenir cualquier implicación negativa.

En todas las actividades relacionadas con las ciencias de la computación, existe un riesgo aceptable, y es necesario analizar y entender estos factores para establecer los procedimientos que permitan analizarlos al máximo y en caso que ocurran, poder reparar el daño y reanudar la operación lo mas rápidamente posible.

En una situación ideal, se deberían elaborar planes para manejar cualquier contingencia que se presente.

Analizando cada aplicación se deben definir planes de recuperación y reanudación, para asegurarse que los usuarios se vean afectados lo menos posible en caso de falla o siniestro. Las acciones de recuperación disponibles a nivel operativo pueden ser algunas de las siguientes:

- En algunos casos es conveniente no realizar ninguna acción y reanudar el proceso.
- Mediante copias periódicas de los archivos se puede reanudar un proceso a partir de una fecha determinada.
- El procesamiento anterior complementado con un registro de las transacciones que afectaron a los archivos permitirá retroceder en los movimientos realizados a un archivo al punto de tener la seguridad del contenido del mismo a partir de él reanudar el proceso.
- Analizar el flujo de datos y procedimientos y cambiar el proceso normal por un proceso alterno de emergencia.
- Reconfigurar los recursos disponibles, tanto de equipo y sistemas como de comunicaciones.

Cualquier procedimiento que se determine que es el adecuado para un caso de emergencia deberá ser planeado y probado previamente.

Este grupo de emergencia deberá tener un conocimiento de los posibles procedimientos que puede utilizar, además de un conocimiento de las características de las aplicaciones, tanto desde el punto técnico como de su prioridad, el nivel de servicio planeado y su influjo en la operación de la organización.

Además de los procedimientos de recuperación y reinicio de la información, se deben contemplar los procedimientos operativos de los recursos físicos como hardware y comunicaciones, planeando la utilización de equipos que permitan seguir operando en caso de falta de la corriente eléctrica, caminos alternos de comunicación y utilización de instalaciones de cómputo similares. Estas y otras medidas de recuperación y reinicio deberán ser planeadas y probadas previamente como en el caso de la información.

En el momento que se hacen cambios o correcciones a los programas y/o archivos se deben tener las siguientes precauciones:
1) Las correcciones de programas deben ser debidamente autorizadas y probadas. Con esto se busca evitar que se cambien por nueva versión que antes no ha sido perfectamente probada y actualizada.
2) Los nuevos sistemas deben estar adecuadamente documentos y probados.
3) Los errores corregidos deben estar adecuadamente documentados y las correcciones autorizadas y verificadas.

Los archivos de nuevos registros o correcciones ya existentes deben estar documentados y verificados antes de obtener reportes.

Procedimientos de respaldo en caso de desastre

Se debe establecer en cada dirección de informática un plan de emergencia el cual ha de ser aprobado por la dirección de informática y contener tanto procedimiento como información para ayudar a la recuperación de interrupciones en la operación del sistema de cómputo.

El sistema debe ser probado y utilizado en condiciones anormales, para que en casó de usarse en situaciones de emergencia, se tenga la seguridad que funcionará. La prueba del plan de emergencia debe hacerse sobre la base de que la emergencia existe y se ha de utilizar respaldos.

Se deben evitar suposiciones que, en un momento de emergencia, hagan inoperante el respaldo, en efecto, aunque el equipo de cómputo sea aparentemente el mismo, puede haber diferencias en la configuración, el sistema operativo, en disco etc.

El plan de emergencia una vez aprobado, se distribuye entre personal responsable de su operación, por precaución es conveniente tener una copia fuera de la dirección de informática.
En virtud de la información que contiene el plan de emergencia, se considerará como confidencial o de acceso restringido.

La elaboración del plan y de los componentes puede hacerse en forma independiente de acuerdo con los requerimientos de emergencia, La estructura del plan debe ser tal que facilite su actualización.

Para la preparación del plan se seleccionará el personal que realice las actividades claves del plan. El grupo de recuperación en caso de emergencia debe estar integrado por personal de administración de la dirección de informática, debe tener tareas específicas como la operación del equipo de respaldo, la interfaz administrativa.
Los desastres que pueden suceder podemos clasificar así:
a) Completa destrucción del centro de cómputo,
b) Destrucción parcial del centro de cómputo,
c) Destrucción o mal funcionamiento de los equipos auxiliares del centro de cómputo (electricidad, aire, acondicionado, etc.)
d) Destrucción parcial o total de los equipos descentralizados
e) Pérdida total o parcial de información, manuales o documentación
f) Pérdida del personal clave
g) Huelga o problemas laborales.

El plan en caso de desastre debe incluir:

La documentación de programación y de operación.
Los equipos:

- El equipo completo
- El ambiente de los equipos
- Datos y archivos papelería y equipo accesorio
- Sistemas (sistemas operativos, bases de datos, programas).

El plan en caso de desastre debe considerar todos los puntos por separado y en forma integral como sistema. La documentación estará en todo momento tan actualizada como sea posible, ya que en muchas ocasiones no se tienen actualizadas las últimas modificaciones y eso provoca que el plan de emergencia no pueda ser utilizado.

Cuando el plan sea requerido debido a una emergencia, el grupo deberá:

- Asegurarse de que todos los miembros sean notificados,
- Informar al director de informática,
- Cuantificar el daño o pérdida del equipo, archivos y documentos para definir que parte del plan debe ser activada.
- Determinar el estado de todos los sistemas en proceso,
- Notificar a los proveedores del equipo cual fue el daño,
- Establecer la estrategia para llevar a cabo las operaciones de emergencias tomando en cuenta:
- Elaboración de una lista con los métodos disponibles para realizar la recuperación
- Señalamiento de la posibilidad de alternar los procedimientos de operación (por ejemplo, cambios en los dispositivos, sustituciones de procesos en línea por procesos en lote).
- Señalamiento de las necesidades para armar y transportar al lugar de respaldo todos los archivos, programas, etc., que se requieren.
- Estimación de las necesidades de tiempo de las computadoras para un periodo largo.

Cuando ocurra la emergencia, se deberá reducir la carga de procesos, analizando alternativas como:

- Posponer las aplicaciones de prioridad más baja,
- Cambiar la frecuencia del proceso de trabajos.
- Suspender las aplicaciones en desarrollo.

Por otro lado, se debe establecer una coordinación estrecha con el personal de seguridad a fin de proteger la información.

Respecto a la configuración del equipo hay que tener toda la información correspondiente al hardware y software del equipo propio y del respaldo. Deberán tenerse todas las especificaciones de los servicios auxiliares tales como energía eléctrica, aire acondicionado, etc. a fin de contar con servicios de respaldo adecuados y reducir al mínimo las restricciones de procesos, se deberán tomar en cuenta las siguientes consideraciones:

- Mínimo de memoria principal requerida y el equipo periférico que permita procesar las aplicaciones esenciales.
- Se debe tener documentados los cambios de software.
- En caso de respaldo en otras instituciones, previamente se deberá conocer el tiempo de computadora disponible.

Es conveniente incluir en el acuerdo de soporte recíproco los siguientes puntos:

- Configuración de equipos.
- Configuración de equipos de captación de datos.
- Sistemas operativos.
- Configuración de equipos periféricos.

2.4 Análisis preliminar del sistema de control de seguridad en base de datos

Como se mencionó en el capítulo I, la planeación constituye una diferencia en el desempeño de una organización, y aún más, si en una de las partes más delicadas de una organización como es la seguridad, no se tomara en cuenta, el mal funcionamiento de la organización dará como resultado

- Incidentes de carácter informático que pueden causar perdida de información valiosa para la empresa.
- Fraudes que se traducen en fugas de información que pueden ser ventaja para otras organizaciones que tengan la misma actividad empresarial.
- Pérdida de ingresos por el mal manejo de la información.

Esta situación se hace aún más preocupante si se tiene en cuenta que pocas empresas contemplan el espectacular incremento del número de conexiones de usuarios, y que las

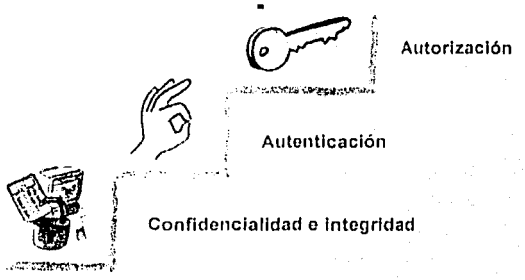
TESIS CON
FALLA DE ORIGEN

conexiones remotas de los medios no sólo aumenta las posibilidades del negocio, sino también, la facilidad para abusar de sus sistemas.

Garantizar la seguridad en los sistemas informáticos es de vital importancia para asegurar el éxito del negocio. Debe aplicarse a cada capa de información y con los distintos niveles de protección que garanticen la autenticidad del interlocutor y la autorización en el acceso a datos y a aplicaciones, así como la confidencialidad e integridad de los mismos. El equilibrio entre este tipo de seguridad y los costes asociados, desde el punto de vista de inversión económica y agilidad en el uso, parece muy difícil de conseguir.

Históricamente, se ha dado mayor importancia a la confidencialidad que a la integridad y autenticidad de los datos, dejándose sin abordar otros aspectos importantes como la autorización o control de acceso y la disponibilidad.

La nueva realidad implica un cambio en el orden de prioridades. El énfasis se pone ahora en la autenticidad e integridad de los datos por encima del resto de aspectos.



2.5 Los aspectos de la seguridad en su jerarquía

La confidencialidad e integridad

Las organizaciones en algunos casos no perciben que la inseguridad da como freno el éxito del negocio, desatendiendo este aspecto en sus sistemas. Desde este punto de vista, es importante hablar no sólo de la necesidad de mejorar las medidas de seguridad exigidas por los procesos que hacen transacciones importantes en los sistemas de una organización, sino también las que se refieren al sistema de autorización.

La autenticación y autorización

La identificación de los usuarios en la base de datos, base de cualquier sistema de autorización, se queda en entredicho con la aparición de nuevas tecnologías. Existen programas capaces de adivinar las contraseñas correctas en cuestión de minutos o, a lo sumo, días. La apertura de éste tipo de tecnología obliga a revisar los sistemas y, en muchos casos, a cambiarlos.

TESIS CON
FALLA DE ORIGEN

El sistema propuesto considera algoritmos de criptográficos. El uso de técnicas criptográficas tiene como propósito prevenir algunas faltas de seguridad en un sistema computarizado.

La palabra criptografía proviene del griego kryptos, que significa esconder y gráphein, escribir, es decir, escritura escondida. La criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas lo puedan entender el mensaje.[1]

Criptográficos comunes comprenden la transposición, substitución y transformación, o una combinación de las tres. Un sistema útil de transformación de datos es aquél cuyos procesos de codificación y descifrado son recíprocamente inversos.

Este sistema implica la adición de un bit a cada bit transmitido. La serie de bits añadidos se substrae del texto transmitido para obtener el mensaje original.

Alguien que quiere mandar información confidencial aplica técnicas criptográficas para poder "esconder" el mensaje (lo llamaremos cifrar o encriptar), manda el mensaje por una línea de comunicación que se supone insegura y después solo el receptor autorizado pueda leer el mensaje "escondido" (lo llamamos descifrar o desencriptar).

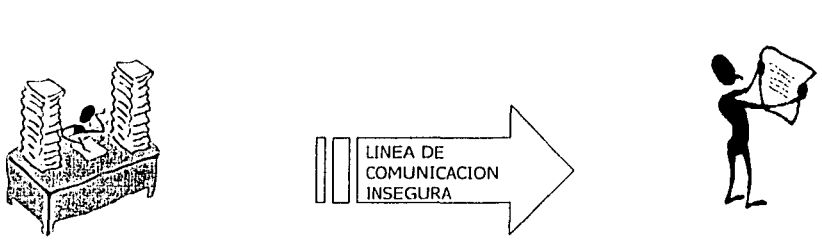


Fig. 2.6 Ciclo de la información al usar técnicas criptográficas

Para poder entender un poco de la criptografía, es tiempo de plantear que tipo de problemas resuelve ésta. Los principales problemas de seguridad que resuelve la criptografía son:

- Privacidad.
- Integridad.
- Autenticación y el no rechazo.

La privacidad, se refiere a que la información sólo pueda ser leída por personas autorizadas. Ejemplos: Si la comunicación se establece por teléfono y alguien intercepta la comunicación o escucha la conversación por otra línea podemos afirmas que no existe privacidad. Si mandamos una carta y por alguna razón alguien rompe el sobre para leer la carta, podemos decir que se ha

[1] John G. Burch, Jr "Sistema de información teoría y práctica" Ed. Limusa 1986 Pag. 380

TESIS CON
FALLA DE ORIGEN

violado la privacidad. En la comunicación por Internet es muy difícil estar seguros que la comunicación es privada, ya que no se tiene control de la línea de comunicación.

Por lo tanto si ciframos (escondemos) la información cualquier intercepción no autorizada no podrá entender la información confidencial. Esto es posible si se usan técnicas criptográficas, en particular la privacidad se logra si se cifra el mensaje con un método simétrico.

La integridad, se refiere a que la información no pueda ser alterada en el transcurso de ser enviada.

Esto también se puede solucionar con técnicas criptográficas particularmente con procesos simétricos o asimétricos. La integridad es muy importante por ejemplo en las transmisiones militares ya que un cambio de información puede causar graves problemas.

La autenticidad, se refiere a que se pueda confirmar que el mensaje recibido haya sido mandado por quien dice lo mando o que el mensaje recibido es el que se esperaba.

Ejemplos: las técnicas necesarias para poder verificar la autenticidad tanto de personas como de mensajes usando quizá la más conocida aplicación de la criptografía asimétrica que es la firma digital, y de algún modo reemplaza a la firma autógrafa que se usa comúnmente, para autenticar mensajes se usa criptografía simétrica.

Por internet es muy fácil engañar a una persona con quien se tiene comunicación respecto a la identidad, resolver este problema es por lo tanto muy importante para efectuar comunicación confiable.

El no rechazo, se refiere a que no se pueda negar la autoría de un mensaje enviado.

Información
Persona Autorizada

Segura

Cuando se diseña un sistema de seguridad una gran cantidad de problemas puedes ser evitados si se ponen en función de comprobar autenticidad, de garantizar privacidad, de asegurar integridad y evitar el no-rechazo.

TESIS CON
FALLA DE ORIGEN

Políticas de seguridad

Además de implementar éstas técnicas de autenticidad, para poder atacar y prevenir todo tipo de anormalidades en la información de los sistemas usados por la empresa es necesario hacer una reestructuración de políticas para la solución del problema de seguridad en la base de datos usada por los sistemas de la organización. Estas políticas estarán basadas en el hecho de mantener las transacciones que alteren a la información completamente seguras.

Además, se tiene que hacer una evaluación del personal autorizado que maneja las operaciones más delicadas de los sistemas de la organización, para que su desempeño en el trabajo sea totalmente profesional y con una ética personal considerable.

Cuidar los procesos que hacen la parte medular del negocio es un aspecto que se debe de considerar para el buen funcionamiento del negocio, esto se puede hacer coordinándose las área de desarrollo de sistemas y el área de operaciones, Existen aspectos en los cuales los desarrolladores tienen conocimiento de las eventualidades que pueden ocurrir, y que es necesario comunicarlas a las personas encargadas de la operación de los sistemas para que sepan como resolverlas.

Política global de seguridad

Se debe de establecer el estatus de la información para la empresa o la organización, debe de contener un objetivo general, la importancia de la tecnología de la información para la empresa, el periodo de tiempo de validez de la política, los recursos con que se cuenta, objetivos específicos de la empresa.

Debe de establecerse la calidad de la información que se maneja según su objetivo, la calidad que debe tener la información quiere decir que se establezca cuando o para quien la información debe ser confidencial, cuando debe verificarse su integridad y cuando debe de verificarse su autenticidad tanto de la información como de los usuarios.

Análisis de riesgos

Consiste en enumerar todo tipo de riesgos a los cuales esta expuesta la información y cuales son las consecuencias, los posibles atacantes entre persona empresas y dependencias de inteligencia, las posibles amenazas etc., enumerar todo tipo de posible perdida desde perdidas directas como dinero, clientes, tiempo etc., así como indirectas: créditos, perdida de imagen, implicación en un litigio, perdida de imagen, perdida de confianza etcétera.

El riesgo se puede calcular por la formula riesgo = probabilidad ×perdida, por ejemplo el riesgo de perder un contrato por robo de información confidencial es igual a la probabilidad de que ocurra el robo multiplicado por la perdida total en pesos de no hacer el contrato.

El riesgo de fraude en transacciones financieras es igual a la probabilidad de que ocurra el fraude por la perdida en pesos de que llegara ocurrir ese fraude. Si la probabilidad es muy pequeña el riesgo es menor, pero si la probabilidad es casi uno, el riesgo puede ser casi igual a la perdida total.

Si por otro lado la perdida es menor aunque la probabilidad de que ocurra el evento sea muy grande tenemos un riesgo menor. Por ejemplo la perdida de una transacción de 300 pesos con una probabilidad muy grande de que ocurra al usar criptografía débil, el riesgo llega a ser menor. En el análisis de riesgo debe también incluirse los posibles ataques que puedan existir y su posible efectos.

Política entorno a los accesos

Identificación de Usuarios

Para poner en marcha el sistema, es necesario establecer algunas políticas de identificación de usuarios, éstas políticas son las siguientes:

- Los usuarios no deberán nunca compartir sus identificaciones como usuarios y sus claves o contraseñas. Cada nuevo usuario debe ser solicitado y justificado al responsable de sistemas y una vez aprobado, deberá ser canalizado a través del Administrador de seguridades para su asignación y control respectivo.

- Es importante que el responsable de sistemas informe tanto al solicitante como al administrador de seguridades, cuales son los tipos accesos que tendrá el nuevo usuario, así como también los no accesos, los cuales inclusive podría abarcar hasta restricciones al nivel de terminales.

- Ningún usuario puede crearse sin su correspondiente clave o contraseña (password) ya que este constituye el único medio de control de seguridades.

- Las claves deben consistir como mínimo de 6 caracteres alfanuméricos (números y letras), los cuales serán elegidos por el usuario. En otras ocasiones y dependiendo de los recursos a los que se tendrá acceso, las claves son asignadas directamente por el Administrador de seguridades e informadas al usuario.

- Es importante que el administrador de usuarios no tenga dentro de sus registros la misma clave para otros usuarios. De producirse este caso, deberá cambiarse la clave inmediatamente e informado al usuario respectivo de la nueva clave. También debe en este caso tomar en cuenta los siguientes factores:

  - No deben existir claves de diferentes usuarios con caracteres iguales en las mismas posiciones, ejm: 123SRRG y 123LRRG.
  - Debe estipularse la cantidad de caracteres numéricos a usarse en la clave.
  - Debe estipularse la cantidad máxima de caracteres.

- Las claves deberán ser cambiadas mínimo cada 30 días. Para los casos de claves de usuarios altamente sensitivos deberá evaluarse un tiempo mayor de cambio.

- Los intentos fallidos deberían ser máximo en un total de tres con clave incorrecta. Cumplidos los tres intentos fallidos, el usuario debe quedar inhibido. Estos intentos deben quedar registrados en el sistema para su posterior control.

- Las claves no deben visualizarse. Su almacenamiento debe ser en forma encriptada (codificada).

- Cada acceso a cada recurso debe contener una clave específica y no repetirse.

- Si el usuario considera el cambio de su clave por perdida de su confidencialidad, debe solicitar al Administrador de seguridad, la asignación de una nueva clave inmediatamente.

- El sistema contiene usuario y clave por default (defecto) para facilitar su instalación. Esta debe cambiarse una vez que el programa haya sido instalado.

- Las claves deben respaldarse en sobres de seguridad y deberán realizarse pruebas aleatorias para verificar su autenticidad y actualidad.

Suspensión de permisos

Los permisos deben ser suspendidos por las siguientes causas:

- Cuando los empleados se ausenten por Vacaciones.

- Cuando su usuario y clave no haya sido utilizado por un lapso de 30 días.

- A evaluación del Administrador de seguridades y Responsable de Sistemas por accesos en fines de semana y feriados.

- Cuando supere los intentos máximos de accesos fallidos a recursos asignados o no.

En cualquiera de estos casos se debe analizar e investigar los motivos y para rehabilitar el usuario, deberán solicitarse las autorizaciones nuevamente, dependiendo del tipo de suspensión aplicada. Para el caso de suspensiones por inactividad del sistema, este debe solicitar la re-entrada de la clave nuevamente.

Acceso a Datos

- La información impresa debe clasificarse de acuerdo a su seguridad.

- En caso de accesos fallidos a datos, el sistema debe mantener dicha información en detalle con el nombre del usuario, fecha, aplicación, archivos, etc. A los que se pretendía accesar, así como también el número de intentos.

- De igual forma el sistema debiera llevar un control sobre los intentos exitosos posteriores a varios intentos fallidos. Estos pueden manejarse a través de logs (archivos de actividades cronológicas) de seguridad que deben ser revisados periódicamente por el Administrador de seguridad.

- Las empresas deben diseñar el procedimiento que les permita asegurar con éxito el Control de las seguridades de accesos a datos.

Accesos a Programas y Utilitarios

Los accesos a programas y utilitarios deben estar segmentado de acuerdo al perfil del usuario. La clasificación general es:

- Los usuarios del sistema

- Los programadores del sistema y, Personal de producción.

- Los usuarios del sistema son los que podrán generar transacciones reales, o usar las funciones del sistema en producción. Podrán también accesar a los archivos generados por el sistema producto de las transacciones.

- Los programadores solo deben tener acceso al ambiente de pruebas o desarrollo. No deben tener acceso a transacciones reales o a accesar a funciones del sistema en producción.

- El personal de producción, debe asegurarse que acceda solo a la información definida para cada usuario. Podrá efectuar las tareas definidas para el área de producción pero previniendo el acceso a datos mediante cualquier tipo de herramienta de programación o a través de programas de aplicación.

- Las bibliotecas de los programas y utilitarios deben estar separadas tanto para desarrollo como para producción.

- Es importante que los programas en desarrollo también sean mantenidos a nivel de versión y con los datos de fecha, hora y usuario que lo desarrolló. Es vital mantener al menos la última y penúltima actualización, de esta forma en caso de reversión se podrá ir a cualquiera de las dos últimas versiones.

- En caso de ser necesario, sí se puede permitir el acceso de bibliotecas del ambiente de desarrollo tanto al usuario del sistema como al personal de producción.

- Antes de que un sistema sea pasado a producción debe efectuarse una evaluación del nivel de seguridades que brinda ese programa o utilitario. Es importante que un auditor de sistemas y el responsable de control interno verifique para determinar si el sistema cumple con las especificaciones técnicas y contiene las seguridades y controles adecuados.

- Los cambios que se efectúen posteriores a programas en producción deben efectuarse de acuerdo al control de cambios.

Controles de Aplicación

Los Controles de Aplicación se constituyen en aquellos enfocados a controles por los usuarios y controles por los sistemas. Los controles por los usuarios están dados sobre los datos de entrada, datos fijos, ítems rechazados o en espera, datos de salida. Los controles por los sistemas se enfocan en los datos de entrada, ítems en espera, y sobre el procesamiento.

TESIS CON
FALLA DE ORIGEN

Los controles por los usuarios se refieren a la responsabilidad que el mismo debe tener en la preparación y aprobación de las transacciones (datos de entrada); en la modificación de datos fijos en los archivos maestros y de tablas del sistema responsabilizándose por la integridad y exactitud de los mismos (datos fijos); en el control de las transacciones rechazadas o en suspenso, las cuales deben ser corregidas inmediatamente de acuerdo a su fecha contable (ítems rechazados y en suspenso) y finalmente es el responsable de los errores o desviaciones presentadas y detectadas en los datos de salidas.

Los controles por los sistemas son aquellos que proveen y garantizan que los datos ingresados son digitados íntegramente (datos de entrada); que los ítems rechazados y en suspenso se identifiquen correctamente y se mantengan pendientes de una solución (ítems rechazados y en espera); y finalmente que el sistema posea mecanismos de control del procesamiento para asegurar que la información fue procesada con los archivos de datos correctos y además brindando a través de las diferentes etapas del procesamiento, un seguimiento de la transacción que permita mantener una adecuada evidencia de auditoría (sobre el procesamiento).

Entre los diferentes controles por los sistemas se pueden citar los de entrada de datos, los cuales están dados mediante la generación de controles por transacciones, controles por totales, controles por secuencia, controles por tamaño de registro, verificación de clave, etc. Estos controles no deben ser seleccionados sino mas bien aplicados todos, ya que tienen una función específica durante todo el trayecto de la operación de entrada.

- Con los Controles por transacciones se establece una aprobación de la misma antes de su procesamiento, esto en aprobaciones automatizadas.
- Para aprobaciones manuales es preferible que esta sea dada al final del procesamiento o cuando la transacción ya está completa, ejm.: Cuando se efectúa un ingreso de una compra en el sistema de compras y la aprobación del pago de la misma se realiza antes de dicho ingreso al sistema, mediante firma en un documento; no se estará seguro de que el ingreso se haya efectuado de forma correcta con las cantidades, proveedor y demás datos de la transacción original. Para evitar fraudes, es importante en este caso aprobar o firmar una vez que la transacción haya sido completada, es decir al final.
- Existe otro tipo de controles que van dirigidos al mantenimiento de la información, respecto de cambios de ítems, precios, cantidades, etc.
- Con los Controles por Totales se establece un registro que asegure que todas las transacciones ingresadas sean totalizadas.
- Los Controles por Secuencia son aquellos que automáticamente o manualmente va generando una secuencia del registro ya sea a nivel de formularios pre-numerados o a través de una secuencia generada automáticamente por documento que se ingresa.
- Los Controles de tamaño de Registro confirman que la longitud del mensaje quede registrada de acuerdo a los parámetros técnicos establecidos y se evite la transmisión de información no contemplada en la transacción. En algunos casos también puede evaluarse la necesidad de transmisión de la información de forma codificada la cual hará más difícil el descifrar la información. Esto último es muy usado cuando la información es altamente sensitiva.
- Los Controles de Aplicación deben en todo caso asegurar que los usuarios acceden o afecten sólo lo autorizado y definido para cada uno de ellos.

TESIS CON
FALLA DE ORIGEN

Control de Actividades del programador de sistemas

Las actividades del programador de sistemas deben asegurarse que el programa diseñado cumpla con los requerimientos solicitados, seguridades e inviolabilidad del caso. El responsable de sistemas se encargará de verificar antes de que el programa sea puesto en producción, de que el programador haya documentado debidamente el programa o cambio, que se hayan efectuado las rutinas de validación y verificación y de que se hayan completado las pruebas del sistema.

Es importante que se realicen verificaciones de las entradas y salidas de datos para todos los registros y que sea imposible la manipulación de algún registro en particular, por ejem.:

Los programadores de aplicaciones bancarias (cuentas corrientes o ahorros) podrían programar débitos o créditos a cuentas sin que estas sean detectadas a simple vista. Es vital que se implante un mecanismo de control y verificación que certifique que el programa en mención cumple con los requerimientos solicitados y las seguridades del caso.

2.5 Diseño funcional y técnico del sistema que Administra la Seguridad

Introducción

El sistema de control de seguridad en base de datos, surge de la necesidad de agilizar y auditar la administración un SISTEMA determinado, correspondiente a la parte de creación de usuarios, y restricciones de los mismos al acceder a determinadas pantallas en un sistema que tiene como plataforma una base de datos.

El sistema de control de seguridad esta diseñado para ser un sistema gráfico y amigable a cualquier persona, por ejemplo:

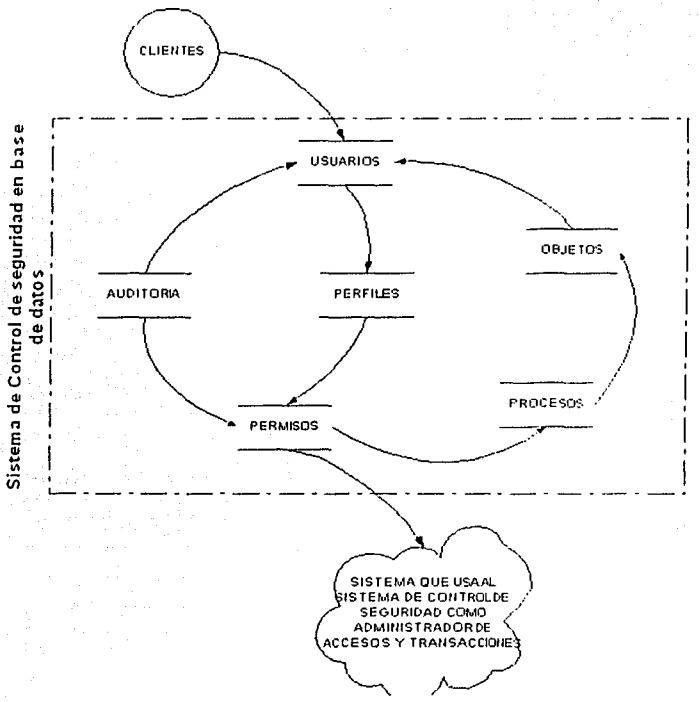
En la parte de los usuarios, se agilizará el proceso al dar de alta, borrar o actualizarlos, ya que no se tendrá que hacer mediante engorrosas instrucciones basadas en SQL si no mediante una simple interfaz gráfica.

Estas tareas de asignación de privilegios podrán ser ejecutadas por el sistema de control de seguridad mediante una pantalla.

Otra característica más del diseño del sistema de control de seguridad de base de datos, es la auditoría de las transacciones y accesos al sistema, es decir que el administrador podrá monitorear o vigilar los movimientos que un determinado usuario lleve acabo en éste, tales como: borrar, actualizar e insertar datos de una manera más eficiente, como en los casos anteriores, utilizando pantallas.

TESIS CON
FALLA DE ORIGEN

Ambiente general



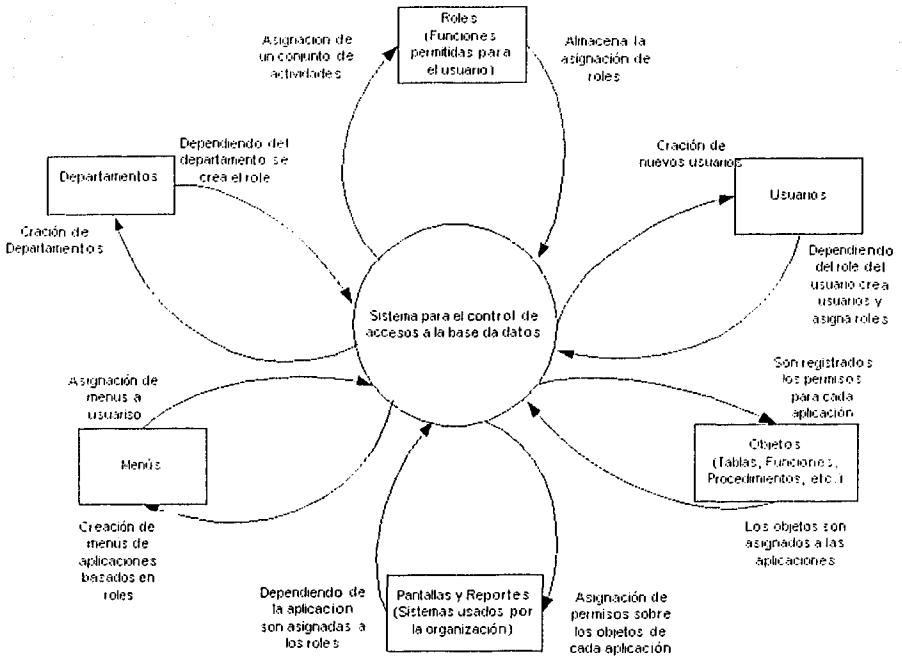
2.7 Marco de operación del sistema de control de seguridad en base de datos[22]

Mediante este sistema de operación, los clientes se registran en el sistema de control de seguridad en base de datos para que dependiendo del perfil asignado puedan operar los sistemas que utilizan la organización.

[22] El sistema de control de seguridad en base de datos es un valor agregado a los sistemas que operan en una organización, el esquema muestra las entidades que involucran y que usa el sistema para tener un control de accesos

TESIS CON
FALLA DE ORIGEN

Diagrama de Contexto



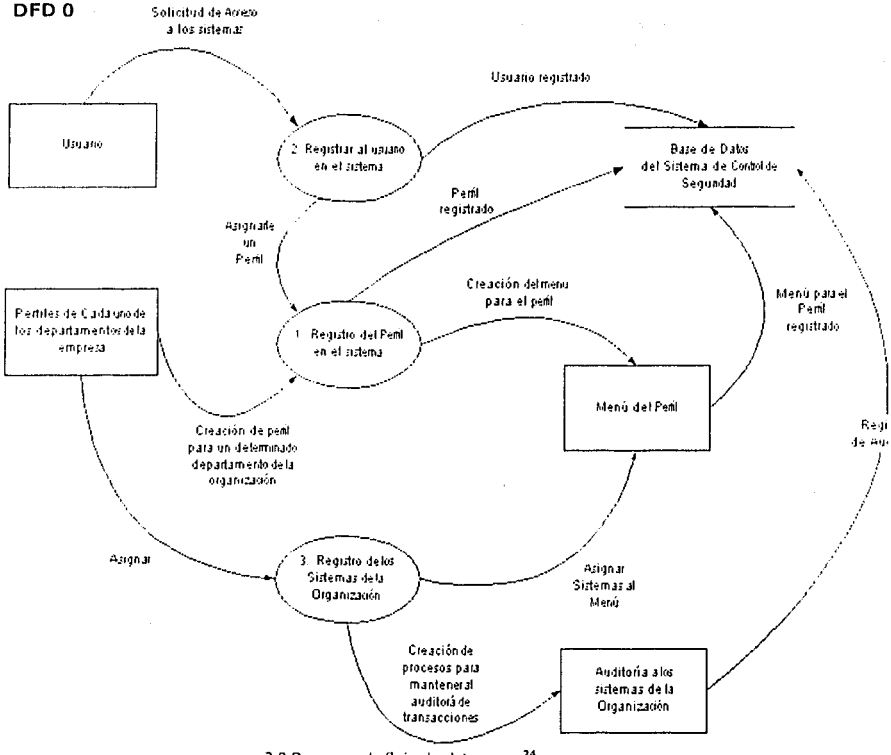
2.8 Diagrama de contexto[23]

Para dar de alta un usuario es necesario primeramente registrar un perfil de acceso (por ejemplo el área de finanzas), posteriormente los usuarios se podrán dar de alta en el sistema de control de seguridad tomando el perfil especificado. Al hacer esta operación el sistema de control de seguridad asignará los procesos que puede ejecutar ese usuario, además los sistemas correspondientes al departamento de su perfil.

El administrador del sistema de control de seguridad podrá modificar los accesos de dicho usuario, podrá agregar sistemas relacionados con su departamento, o revocar accesos. Además podrá ver que transacciones de información, ha hecho con una interfaz gráfica.

[23] Diagrama de contexto del sistema para el control de accesos a la base de datos (Creación propia)

TESIS CON
FALLA DE ORIGEN



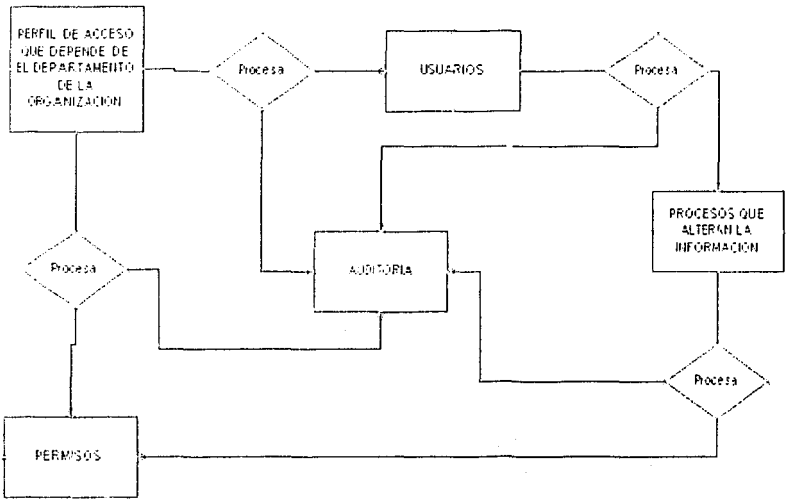
2.9 Diagrama de flujo de datos cero[24]

El DFD 0 es el diagrama general de procedimientos que engloban al sistema de control de accesos y el orden en el cuál deben efectuarse para operar al sistema. Los subprocesos contenidos son los siguientes:

1.- Registro del perfil o role del sistema. Esto es, registrar un role por departamento.
2.- Registrar usuarios del sistema
3.- Registro de los sistemas de la organización. Esto es cargar las aplicaciones al menú dependiendo del perfil de acceso.

[24] Diagrama de flujo de datos para el sistema de control de accesos (Creación propia)

TESIS CON
FALLA DE ORIGEN



2.10 Diagrama de flujo de la información.[25]

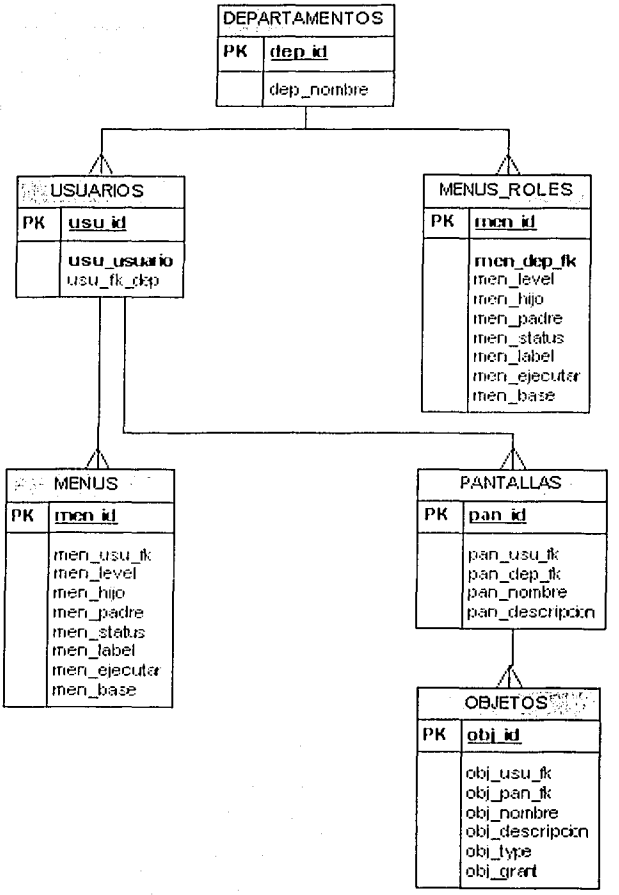
Primeramente se asigna un perfil de acceso a un usuario, a su vez, éstos usuarios hacen transacciones a la información a través de procesos de la base de datos que fueron previamente asignados por el sistema de control de seguridad, los procesos evalúan la seguridad de las transacciones y ejecutan alteraciones de la información a la base.

Cada acción realizada por un usuario en los sistemas de la organización serán registradas en tablas de la base de datos dedicadas a la auditoría.

TESIS CON
FALLA DE ORIGEN

[25] Diagrama de flujo de la información del sistema de control de accesos a la base de datos (creación propia)

Diagrama entidad-relación



2.11 Diagrama entidad relación[26]

[26] Diagrama entidad- relacion del sistema de control de accesos a la base de datos.

TESIS CON
FALLA DE ORIGEN

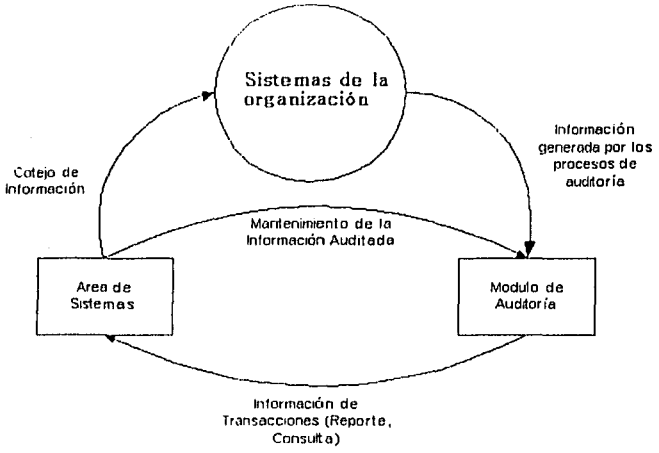
Análisis preliminar de auditoría de transacciones

Introducción

Debido a que se debe tener un control de las transacciones sobre la información de los sistemas de la organización, para hacer evaluaciones periódicas sobre el flujo y modificación de la información, ha surgido la necesidad de implementar un modulo de auditoría de transacciones.

La auditoría de transacciones debe de evaluar el entorno de transacciones de los procesos y aplicaciones que involucran a los sistemas de la organización.

El objetivo de éste módulo es proporcionar al área de sistemas la infraestructura necesaria para consultar los movimientos de la información, así como por quien y que día se hicieron la base de datos que involucra al los sistemas de la organización. Además pretende evaluar la seguridad lógica y flujo de la información únicamente de los objetos que componen la base de datos que almacenará la información de los sistemas.



2.12 Diagrama de contexto del módulo de auditoría.

Mediante el módulo de auditoría el área de sistemas podrá identificar el tipo de transacciones hechas a las tablas de base de datos que involucran a los sistemas de la organización y a su vez podrán cotejarla consultando directamente a la base de datos de auditoría.

TESIS CON
FALLA DE ORIGEN

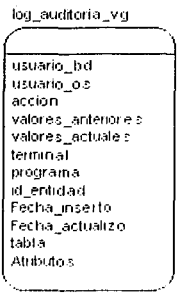
Además, el área de sistemas tendrá que darle mantenimiento a la información almacenada en la tabla de auditoría para que no cresca de volumen indefinidamente.

Esquema de la tabla:

Campo	Tipo Dato	Nulo	Descripción
Usuario_BD	Varchar2(30)	Si	Usuario registrado en la Base de Datos
Usuario_OS	Varchar2(30)	Si	Usuario firmado en el Sistema Operativo
Terminal	Varchar2(16)	Si	Terminal de red usada para efectuar la transacción
Programa	Varchar2(64)	Si	Programa usado para la ejecución de transacción(Forms, sql*plus, etc.)
Accion	Varchar2(15)	Si	DML Realizada (Actualizar, Insertar, Borrar)
Tabla	Varchar2(30)	Si	Tabla de Base de Datos que afecto la transacción
Atributos	Varchar2(30)	Si	Atributo sobre los cuales se están haciendo transacciones
Id_entidad	Varchar2(30)	Si	Atributo común para tablas involucradas en los sistemas de la organización.
Valores_anteriores	Varchar2(32000)	Si	Valores de la tabla, antes de ejecutar una actualización
Valores_actuales	Varchar2(32000)	Si	Valores a los cuales se hizo la transacción
Fecha_inserto	Date	Si	Fecha y hora en que se inserto una transacción
Fecha_actualizo	Date	Si	Fecha y hora en que se actualizo información

TESIS CON
FALLA DE ORIGEN

Estructura



2.13 Estructura de la tabla de auditoría

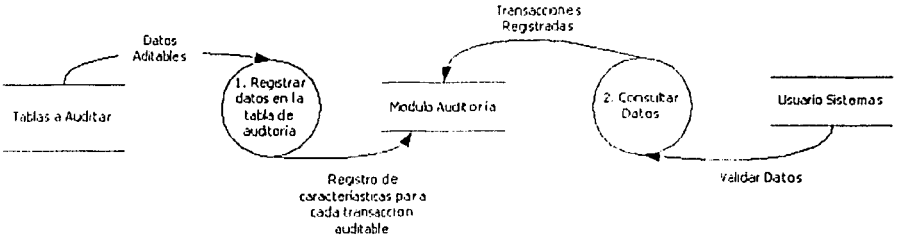
Ejemplo y descripción de datos de la tabla de auditoría

Campo	Ejemplo de Dato	Descripción
Usuario_BD	FOSO	Usuario registrado enla Base de Datos
Usuario_OS	Rubicel_medina	Usuario firmado en el Sistema Operativo
Terminal	MOBIOE09	Terminal de red usada para efectuar la transacción
Programa	TOAD	Programa usado para la ejecución de transacción(Forms, sql*plus, etc.)
Accion	UPDATE	DML Realizada (Update, Insert, Delete)
Tabla	CAT_BANCOS	Tabla de Base de Datos que afecto la transacción
Atributos	BAN_NOMBRE_CORTO - BAN_NOMBRE_LARGO	Atributo sobre los cuales se estan haciendo transacciones. En este caso únicamente se almacenará los campos sobre los cuales se estan haciendo actualizaciones, se formará una cadena en la cual para cada campo estará entre comillas y separando comas
Valores_anteriores	'INVERLAT','BANCO INVERLAT, S.A.'	Valores de la tabla, antes de ejecutar una actualización.Estos valores se almacenarán formando una cadena con los valores se cada campo separados por comillas y comas
Valores_actuales	'B.INVERLAT','BANCO INVERLAT'	Valores a los cuales se hizo la transacción. Estos valores se almacenarán formando una cadena con los valores de cada campo separados por comillas y comas
Fecha_inserto	11-MAY-2003 9:56:00	Fecha y hora en que se inserto una transacción. Este campo será llenado únicamente cuando se lleve acabo una

TESIS CON
FALLA DE ORIGEN

		transacción de inserción sobre las tablas auditadas
Fecha_actualizo	11-MAY-2003 9:56:00	Fecha y hora en que se actualizo Este campo será llenado únicamente cuando se lleve acabo una transacción de actualización sobre las tablas auditadas

DFD 0



2.14 Diagrama de flujo de datos del módulo de auditoría.

El diagrama de flujo de datos descrito en la figura engloba dos procesos:

DFD1. Registrar datos auditables en la tabla de auditoría

DFD2. Consulta de datos a la tabla de auditoría

La raíz del modulo de auditoría es la creación de un trigger[27] de base de datos por cada tabla que se desea auditar.

Este trigger deberá identificar que campos (previamente definidos a auditar) de la tabla fueron actualizados, así como almacenar en la tabla de auditoría los datos anteriores y posteriores a la actualización.

En el caso de borrado de un registro, debe de almacenar los datos que fueron borrados de la tabla en la tabla de auditoría, y por último en el caso de inserción debe de almacenar todos los datos indicados a auditar.

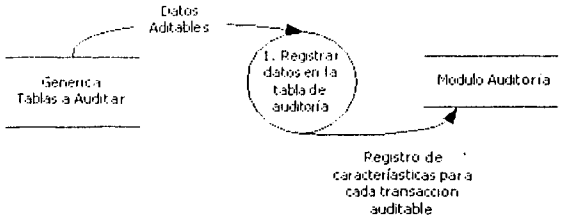
[27] Trigger :- Serie de acciones o procesos que se ejecutan cuando un evento es ejecutado.

TESIS CON
FALLA DE ORIGEN

DFD1 **Registrar datos auditables en la tabla de auditoría**

Se debe crear un trigger de base de datos por cada tabla que se desea auditar. Este trigger debera identificar que campos (previamente definidos) de la tabla fueron actualizados, así como almacenar en la tabla de auditoría los datos anteriores y posteriores a la actualización. En el caso de borrado de un registro, debe de almacentar los datos que fueron borrados de la tabla en la tabla de auditoría, y por último en el caso de inserción debe de almacenar todos los datos indicados a auditar en la misma.

Replicación de transacciones auditadas



2.15 Módulo de registro de datos en la tabla de auditoría

Se debe de almacenar las transacciones para cada campo de las tablas usadas por los sistemas de la organización, en la tabla **log_auditoria_vg** a través de un trigger de base de datos. **Como ya se ha mencionado, se debe de crear un trigger de base de datos por cada tabla a auditar.** Los tipos de transacciones que alteran la información son actualizaciones, borrado o inserción de información en las tablas de la BD. Por tal efecto cada trigger debe de considerar los tres casos.

El nombre de cada trigger de base de datos se formará de la siguiente manera:
Trg_audit_*nombretabla*_vg

Caso Actualización

El trigger de base de datos debe almacenar la siguiente información en la tabla log_auditoria_vg, cada que se actualice un campo de la tabla de bd que se va a auditar.

Campo	Ejemplo de Dato	Descripción
Usuario_BD	FOSO	Usuario registrado en la Base de Datos que realiza la actualización sobre la tabla
Usuario_OS	Rubicel_medina	Usuario firmado en el Sistema Operativo
Terminal	MOBIOE09	Terminal de red usada para efectuar la transacción
Programa	Ifrun60.exe	Programa usado para la ejecución de

TESIS CON
FALLA DE ORIGEN

		transacción(Forms, sql*plus, etc.)
Accion	UPDATE	DML Realizada
Tabla	*"NOMBRE DE LA TABLA AUDITADA"*	Tabla de Base de Datos que efectuó la transacción
Atributos	*'Campo1', 'CAMPO2', 'CAMPO3', 'CAMPO4'*	El trigger de base de datos debe de identificar que campos se están actualizando y cuales deben de ser auditables. Una vez identificando esto en este campo se almacenará una cadena que se compondrá de los nombres de los atributos identificados, entre comillas y separados por comas.
Id_entidad	Valor id entidad	Si la tabla a auditar contiene el campo id_entidad, poenerlo aquí. Este es un atributo común para algunas tablas involucradas en los sistemas de la organización
Valores_anteriores	*'valorcampo1', 'valorcampo2', 'valorcampo3'*	Valores de los atributos la tabla, antes de ejecutar la actualización. Estos valores se almacenarán formando una cadena con los valores de cada campo separados por comillas y comas
Valores_actuales	*'valorcampo1', 'valorcampo2', 'valorcampo3'*	Valores de los atributos a los cuales se hizo la transacción. Estos valores se almacenarán formando una cadena con los valores de cada campo separados por comillas y comas
Fecha_inserto	Null	
Fecha_actualizo	11-MAY-2003 9:56:00	Fecha y hora en que se actualizo Este campo será llenado únicamente cuando se lleve acabo una transacción de actualización sobre las tablas auditadas

Caso Inserción

El trigger de base de datos debe almacenar la siguiente información en la tabla log_auditoria_vg, al insertar un registro:

Campo	Ejemplo de Dato	Descripción
Usuario_BD	FOSO	Usuario registrado en la Base de Datos que realiza la actualización sobre la tabla
Usuario_OS	Rubicel_medina	Usuario firmado en el Sistema Operativo
Terminal	MOBIOE09	Terminal de red usada para efectuar la transacción
Programa	Ifrun60.exe	Programa usado para la ejecución de transacción(Forms, sql*plus, etc.)
Accion	INSERT	DML Realizada
Tabla	*"NOMBRE DE LA TABLA AUDITADA"*	Tabla de Base de Datos que efectuó la transacción
Atributos	*'Campo1', 'CAMPO2',*	Total de atributos o campos contenidos en la tabla. La forma en como se almacenará esto por

TESIS CON
FALLA DE ORIGEN

	'CAMPO3', 'CAMPO4'	medio de una cadena que se compondrá de los nombres de los atributos, entre comillas y separados por comas.
Id_entidad	Valor id entidad	Si la tabla a auditar contiene el campo id_entidad, ponerlo aquí. Este es un atributo común para algunas tablas involucradas en los sistemas de la organización.
Valores_anteriores	*Null*	No hay valores anteriores, por lo que en éste caso el atributo tendrá valor nulo.
Valores_actuales	*'valorcampo1', 'valorcampo2', 'valorcampo3', null, 'valorcampo5', null, 'valorcampo6'*	Valores de los atributos a los cuales se hizo la transacción. Estos valores se almacenarán formando una cadena con los valores de cada campo separados por comillas y comas. En el caso de insertar un registro con datos nulos, éste dato será representado en la cadena con la instrucción "null"
Fecha_inserto	19-MAY-2003 14:59:08	Fecha y hora en que se inserto. Este campo será llenado únicamente cuando se lleve acabo una transacción de inserción sobre las tablas auditadas
Fecha_actualizo	Null	Para el caso de inserción, este atributo debe de tener el valor nulo.

Caso Borrado

El trigger de base de datos debe almacenar la siguiente información en la tabla log_auditoria_vg, al borrar un registro:

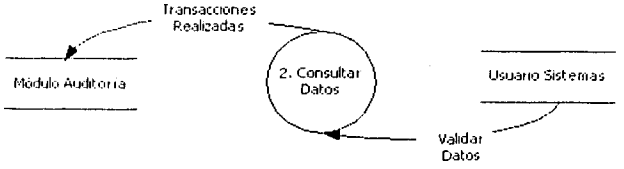
Campo	Ejemplo de Dato	Descripción
Usuario_BD	FOSO	Usuario registrado en la Base de Datos que realiza la actualización sobre la tabla
Usuario_OS	Rubicel_medina	Usuario firmado en el Sistema Operativo
Terminal	MOBIOE09	Terminal de red usada para efectuar la transacción
Programa	ifrun60.exe	Programa usado para la ejecución de transacción(Forms, sql*plus, etc.)
Accion	DELETE	DML Realizada
Tabla	*"NOMBRE DE LA TABLA AUDITADA"*	Tabla de Base de Datos que afectuo la transacción
Atributos	*'Campo1', 'CAMPO2', 'CAMPO3', 'CAMPO4'*	Total de atributos o campos contenidos en la tabla. La forma en como se almacenará esto por medio de una cadena que se compondrá de los nombres de los atributos, entre comillas y separados por comas.
Id_entidad	Valor_id entidad	Si la tabla a auditar contiene el campo id_entidad, ponerlo aquí. Este es un atributo común para algunas tablas involucradas en los sistemas de la

TESIS CON
FALLA DE ORIGEN

		organización.
Valores_anteriores	*valorcampo1,, 'valorcampo2,, 'valorcampo3',*	Valores de los atributos la tabla, antes de ejecutar la actualización. Estos valores se almacenarán formando una cadena con los valores de cada campo separados por comillas y comas.
Valores_actuales	*NULL*	Este atributo para el caso de borrado de registros contendrá un valor nulo.
Fecha_inserto	*NULL*	Este atributo para el caso de borrado de registros contendrá un valor nulo.
Fecha_actualizo	19-Jun-2003 19:54:18	Fecha y hora en que se borro el registro.

DFD2. Consultar Datos

Para poder acceder a la información almacenada en la tabla **log_auditoria_vg** generada por los procesos de auditoría, es necesario crear una interfaz, para que facilite el acceso a la información y el despliegue del reporte.

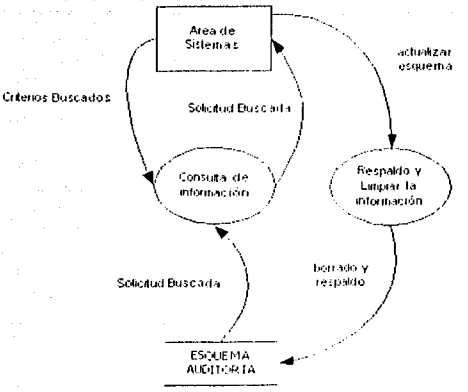


2.16 Módulo de consulta de datos de la información auditada.

Funcionalidad:

- El área de sistemas va a monitorear los movimientos hechos a la base de datos de la organización a través de ésta una interfaz.
- La información almacenada en el esquema de auditoría debe ser limpiada y respaldada por el encargado destinado.
- La interfaz creada para la consulta de la información auditada, no va a poder ser editada ni borrada por ningún usuario.
- La única forma en que se generará la información en el esquema de auditoría es por medio de los procesos que se dispararán cuando se haga alguna transacción.

TESIS CON
FALLA DE ORIGEN



2.17 Diagrama del flujo de consulta de la información auditada.

Pantalla de búsqueda de la información auditada:

Esta pantalla permitirá realizar búsquedas por diversos criterios, la forma en como funcionará, será que se le ingresarán los criterios de búsqueda deseados, y se desplegará en pantalla la información solicitada, si no se ingresa ningún criterio de búsqueda, al pantalla desplegará toda la información existente en la tabla log_auditoria_vg.

La pantalla contará con botones de registro siguiente, registro anterior, primer registro y último registro, para navegar a través de los registros recuperados. Además de el botón de impresión de reporte y de búsqueda

TESIS CON
FALLA DE ORIGEN

2.6 Manual de Operación Administrativo para Controlar y Proveer los Accesos a los Sistemas Informáticos.

Antecedentes

Debido a el constante cambio de usuarios, niveles de acceso y transacciones a la aplicación principal de un sistema de base de datos y para prevenir violaciones de transacciones y de accesos de información a la base de datos principal. Así como auditar las transacciones hechas por los usuarios se diseño este sistema de control de seguridad en base de datos. Actualmente el proceso de asignación de aplicaciones, creación de usuarios, perfiles de acceso, y borrado de los mismos se hace de forma que solo la persona capacitada en este caso en el manejador de base de datos ORACLE puede hacerlo.

El principal objetivo de éste sistema es elaborar el proceso de asignación de aplicaciones y privilegios por perfiles de acceso, mediante un sistema que tenga una interfaz gráfica para la asignación de los mismos y poder visualizar el control del uso de las aplicaciones computacionales de una organización. Además se pretende automatizar la creación, borrado y actualizado de usuarios y perfiles. Además de auditar las transacciones hechas a los sistemas

Introducción

El sistema de control de seguridad en base de datos, surge de la necesidad de agilizar la asignación los accesos a las aplicaciones (Formas, Reportes, Procesos, etc) de una base de datos basado en un menú dinámico. Este menú dinámico solo será manipulado por aquellas personas que sean encargadas de asignar accesos así como de crear, borrar y actualizar usuarios y perfiles para la aplicación principal de una empresa.

- Con esta aplicación se podrá llevar un control estructurado de los objetos que usan cada aplicación, así como de los objetos usados por un usuario y de los usuarios asignados a los perfiles para la aplicación empresarial.
- Se visualizaran los usuarios, perfiles, pantallas, reportes con las características de cada uno por medio de pantallas y procesar reportes con esta información.
- Restringir los accesos a pantallas, reportes o procesos a nivel de usuario
- Personalización del menú para cada usuario o por perfil.
- Poder interactuar directamente con aplicaciones ejecutables de Windows
- Poder interactuar con archivos generados por Windows.

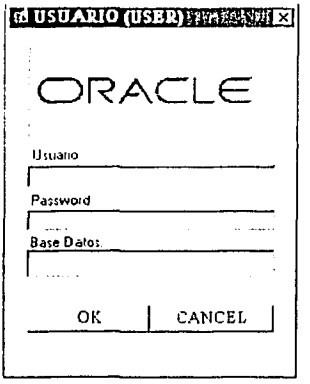
Cada uno de estos objetivos será llevado a cabo en tiempo de ejecución por el sistema.

TESIS CON
FALLA DE ORIGEN

Operación

La forma de conectarse al sistema es por medio de una clave de acceso, un password y la base de datos a la cuál se desea conectar. Como política de seguridad, el sistema pedirá al usuario que cambie su clave de acceso cada inicio de mes, esto reducirá la probabilidad de que un usuario se conecte con la clave que no le corresponda.

Además, como parte del módulo de auditoría de transacciones, el sistema registrará la hora y el día en que el usuario se conecto a los sistemas de la organización. El sistema de control de accesos, a su vez puede ser programado para que los usuarios operen en los horarios de oficina, es decir, solo podrá conectarse un usuario si esta trabajando en su jornada normal de trabajo.



2.18 Pantalla de conexión al sistema.

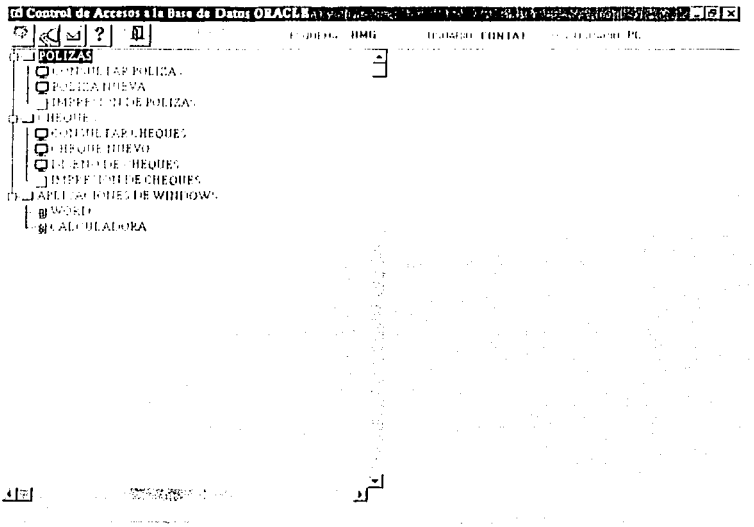
Al hacer la petición de acceso al sistema, la información viaja al servidor de base de datos de forma criptografiada[28], usando la técnica de criptografía "simétrica".

El menú será presentado de la siguiente forma para todos los usuarios de la aplicación. Las aplicaciones y reportes serán presentados de manera distinta a los módulos y submenús, además serán ejecutados haciendo doble clic sobre estos. Los iconos que representarán las formas, reportes y ejecutables de Windows serán de forma distinta para una mejor identificación de los objetos.

El menú será presentado de acuerdo al role o perfil de acceso que le ha sido asignado por el supervisor o encargado del departamento de la organización.

[28] Del griego *kryptos*, que significa esconder y *gráphein*, escribir, es decir, escritura escondida

TESIS CON
FALLA DE ORIGEN



2.19 Pantalla de inicio para operar las aplicaciones de base de datos de la organización.

Los nodos principales serán los módulos de la aplicación y las ramificaciones presentarán los submenus. Estos módulos y submenus, tendrán la funcionalidad normal de un árbol de windows.

Además esta pantalla presentará el esquema al cuál esta conectado el usuario, el usuario de base de datos y el usuario del sistema operativo.

ESQUEMA: **RMG** USUARIO **CONTA1** O S USUARIO **PC**

Funcionalidad de la barra de botones.

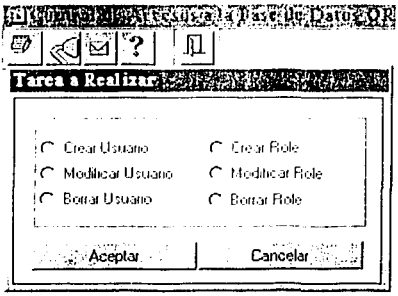
Edición.- Solo será habilitado para los usuarios autorizados a modificar el menú. Sirve para llamar a las funciones de crear usuario, modificar usuario, borrar usuario, crear role, modificar role, y/o eliminar role.	
Conexión.- Es usado para que presente la pantalla de conexión a los sistemas, y el usuario pueda reconectarse sin tener que dar por finalizada la sesión y reiniciar nuevamente el sistema para conectarse	

TESIS CON
FALLA DE ORIGEN

Correo electrónico.- Sirve para mandar mensajes de correo electrónico entre los usuarios del sistema.	
Ayuda.- Manda a ejecutar una ayuda para el uso de los sistemas de la organización.	
Salir.- Abandona la sesión del usuario en el sistema.	

Edición y configuración del sistema de control de accesos a la base de datos

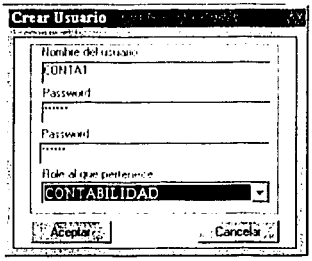
Al dar clic sobre este botón de editar será desplegado el siguiente menú de opciones:



2.20 Opciones de edición al sistema.

Crear Usuarios

Al posicionar el foco del cursor en la opción de "Crear usuario" y oprimir el botón Aceptar, será desplegada la siguiente ventana:

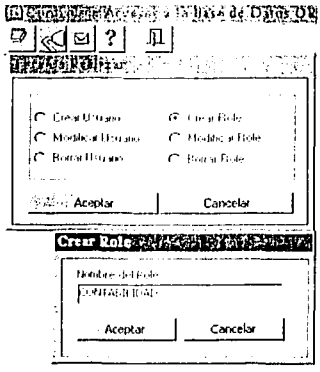


2.21 Ventana para la creación de usuarios

TESIS CON
FALLA DE ORIGEN

En el campo de "Nombre de usuario", se debe de indicar el usuario de la base de datos, esta cadena será la que será requerida cada que el nuevo usuario se identifique. En el campo password debe de indicar el password con el que el usuario de la base de datos entrará al sistema por vez primera, ya que ese momento el sistema identificará que estará entrando por vez primera y le solicitará que cambie esta cadena. El siguiente campo también llamado password, sirve para ratificar la cadena de password indicada. En el campo "Role al que pertenece" será indicado el departamento al que pertenece el nuevo usuario, esto es una especie de plantilla inicial de operación de sistemas del departamento, aunque se puede personalizar individualmente el menú de cada usuario. Al indicar los datos del nuevo usuario, será registrado en la base de datos y en la tabla de usuarios.

Crear role o perfil de acceso: En el desarrollo del sistema, se crea un role o perfil por departamento de la organización. Al posicionar el foco del cursor en la opción "Crear role" y oprimir el botón Aceptar, será desplegada la siguiente ventana:



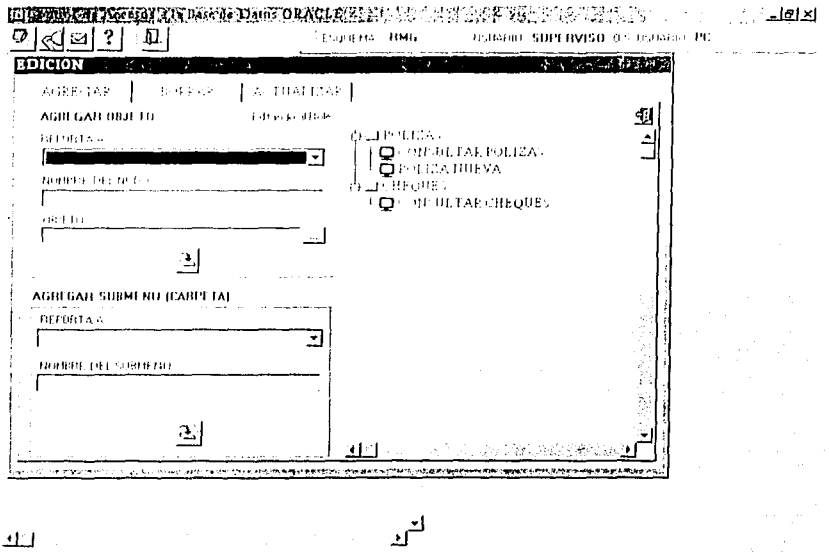
2.22 Módulo de creación de roles

En la ventana de "Crear role" se indica el nombre del role a crear, al oprimir el botón aceptar, se crea un perfil de acceso para los sistemas de la organización. Este role es registrado en la base de datos por el manejador de la base de datos y por el esquema de seguridad.

Este role podrá ser editato inmediatamente después de oprimir el botón aceptar, los accesos que tendrá el role además de ser por aplicación, es por objeto de base de datos (procedimientos, tablas, vistas, funciones, etc.). Es decir por cada aplicación asignada al role, serán asignados los objetos de base de datos que la función use.

Inmediatamente después de generar el role, se desplegará la pantalla de edición del role:

TESIS CON
FALLA DE ORIGEN



2.23 Edición de role o perfil de usuarios

Por medio de esta pantalla se crea un menú de acceso a aplicaciones y reportes de los sistemas de la organización para el perfil de acceso que se esta procesando. El menú es una plantilla de accesos a los sistemas, ya que además de poder asignar este menú a los usuarios, se podrá personalizar para cada uno.

En el apartado de "Crear submenú o carpeta", se crea un módulo o submódulo para asociar objetos de tipo aplicaciones, reportes o aplicaciones de windows. En el apartado "Agregar objeto", se asocia una aplicación a una modulo o submódulo previamente creado.

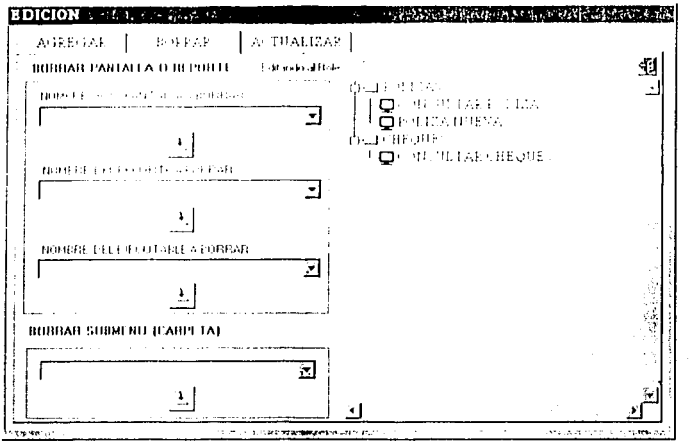
Las pestañas indicadas en la parte superior "Borrar" y "Actualizar", actualizan los módulos y aplicaciones asignadas para el perfil de acceso.

Modificar role o perfil de acceso

Al elegir la opción "Modificar role" se despliega la ventana presentada en la figura 2.20, con esto se puede editar el menú para el role o perfil de acceso indicado.

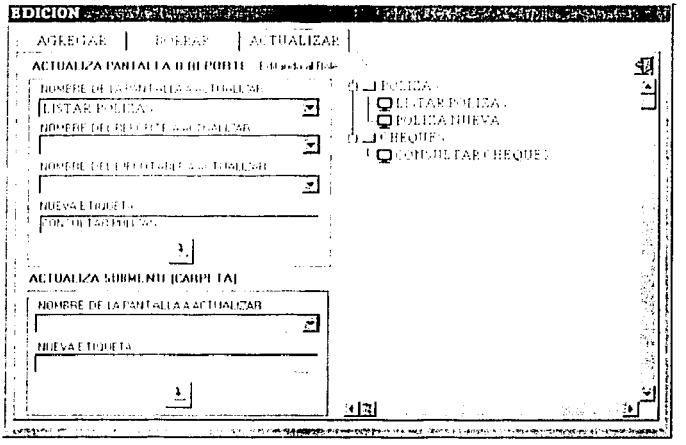
El menú cambiará para los usuarios asociados a el role en las funciones que serán editadas, pero el menú del usuario conservará las demás opciones personalizadas por cada usuario.

TESIS CON
FALLA DE ORIGEN



2.24 Opción borrar nodos del árbol del menú asignado al role.

La figura 2.21 muestra la manera en como se puede borrar una pantalla, reporte, ejecutable o submenú del menú asociado al role que se esta editando. La figura 2.22 muestra la forma en como se pueden actualizar las etiquetas de los objetos o submenús asociados al role.

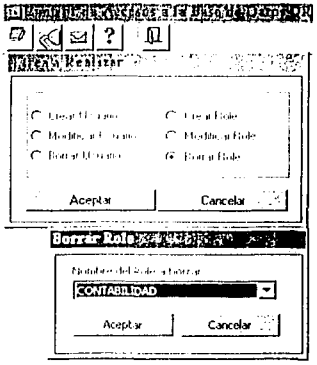


2.25 Actualización de etiquetas de las pantallas, reportes, submódulos

TESIS CON
FALLA DE ORIGEN

Borrar role

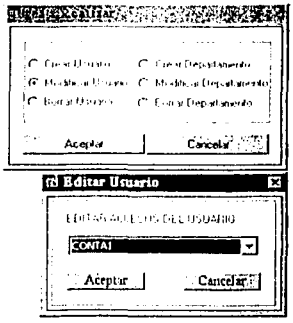
Al elegir la opción borrar role, se borra el perfil de acceso indicado. Cabe señalar que al borrar el role, serán borrados todos los accesos para los usuarios asociados a ese perfil de acceso.



2.26 Borrar el role asociado al departamento

Modificar usuarios

Al indicar el radio-botón de automáticamente se llenarán los dos campos de listas, una de "Roles" y el otro de "Usuarios Existentes". Al seleccionar el usuario a modificar e indicar el botón de aceptar se desplegará una pantalla para poder editar el menú de sistemas del usuario seleccionado. Además con esta opción, también será posible cambiar el password que el usuario tiene asignado.

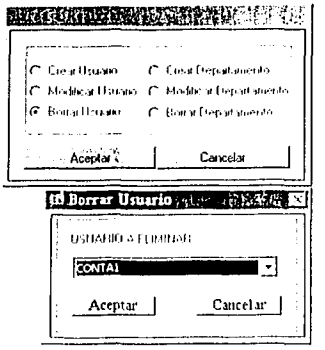


2.27 Editar los accesos del usuario seleccionado

TESIS CON
FALLA DE ORIGEN

Borrar usuario

Por último la opción borrar usuario, borra al usuario con todos los accesos que tenga asociados.



2.28 Borrar el usuario de la base de datos

Funciones de Auditoría

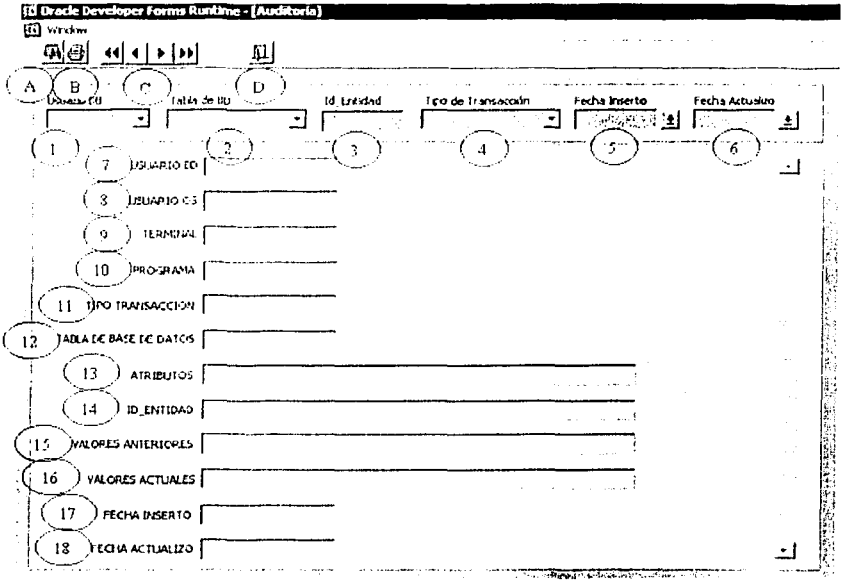
Pantalla de consulta de información concerniente a la auditoría

Descripción de cada uno de los campos de la pantalla de consulta de información auditada por los sistemas:

Número de ITEM	Descripción	Funcionalidad
A	Botón de Búsqueda	Una vez que el usuario ingresa los criterios de búsqueda, al oprimir el botón, se recuperará la información solicitada
B	Botón de despliegue del reporte	Al oprimir el botón, el reporte es desplegado en pantalla dependiendo de los criterios de búsqueda que se encuentren en la pantalla, si no se encuentra ningún criterio de búsqueda el reporte desplegará todo lo contenido en la tabla Log_auditoria_vg
C	Botones de navegación	Por medio de éstos botones se puede navegar a través de los registros recuperados en el bloque detalle
D	Botón de Salida	Botón que se sale de la aplicación
1	Campo de búsqueda del usuario de Base de Datos	Ingresando el usuario de base de datos recupera todas las transacciones hechas por ese usuario
2	Tabla de Base de Datos	Ingresando la tabla de base de datos recupera las transacciones hechas a esas tablas
3	Id_entidad	Obtiene todas las transacciones hechas para dicha entidad
4	Tipo de transacción	Obtiene las transacciones, ya sea de insert, update o delete

TESIS CON
FALLA DE ORIGEN

5	Fecha de inserción	Recupera las transacciones para la fecha de inserción indicada
6	Fecha actualización	Recupera las transacciones para la fecha de actualización indicada
7, 8, 9,10,11,12 ,13,14,15, 16,17,18	Campos detalle	Estos campos son los atributos correspondientes a la tabla log_auditoria_vg



2.29 Pantalla de consulta de información auditada

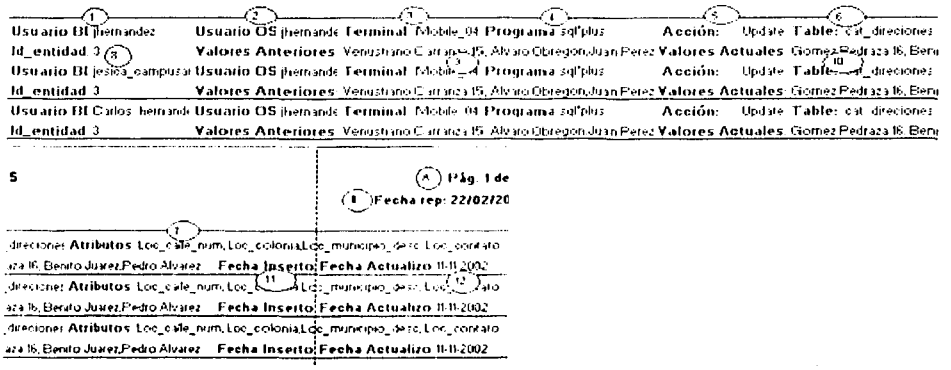
Reporte de auditoría de transacciones

Campo	Tabla DB	Campo DB	Descripción
A	----------	----------	Número de página del reporte
B	----------	----------	Fecha del reporte, SYSDATE
1	Log_auditoria_vg	Usuario_db	Usuario registrado de la base de datos
2	Log_auditoria_vg	Usuario_OS	Usuario de Red
3	Log_auditoria_vg	Terminal	Terminal usada para efectuar la transacción

TESIS CON
FALLA DE ORIGEN

4	Log_auditoria_vg	Programa	Programa usado para la ejecución de transacción(Forms, sql*plus, etc.)
5	Log_auditoria_vg	Accion	Tipo de transacción realizada
6	Log_auditoria_vg	Tabla	Tabla de base de datos que efectuó la transacción
7	Log_auditoria_vg	Atributos	Atributo sobre las cuales se están haciendo transacciones
8	Log_auditoria_vg	Id_entidad	Atributo común para tablas involucradas en los sistemas de la organización
9	Log_auditoria_vg	Valores_anteriores	Valores de la tabla, antes de ejecutar una actualización
10	Log_auditoria_vg	Valores_actuales	Valores a los cuales se hizo la transacción
11	Log_auditoria_vg	Fecha_inserto	Fecha y hora en que se inserto una transacción
12	Log_auditoria_vg	Fecha_actualizo	Fecha y hora en que se actualizo información

Auditoria de Transacciones



2.30 Reporte de auditoria de transacciones

Conclusiones Capitulo II

En el primer apartado de éste capítulo se hace hincapié en que la buena planeación para el control de seguridad es un elemento clave para que los sistemas desarrollados, mantengan la información confidencial, integra y disponible. Además, se propone una metodología para la definición de estrategias de seguridad, esta metodología ayuda en un 90% de los casos a que no se corrompa la información almacenada en las bases de datos y en caso de alguna contingencia, se establecen estrategias reactivas y preactivas que reducen en un 30% la pérdida de la información en el caso de algún incidente informático

Por lo mencionado en el apartado 2.2 (estudio del análisis estructurado), se concluye que ésta técnica sirve de manera fundamental para el desarrollo de los sistemas de información, por lo que el sistema de control de seguridad en bases de datos funda el desarrollo de su infraestructura en esta metodología.

En la sección 2.3 se proponen políticas, procedimientos y prácticas de control de datos para evaluar el ambiente de seguridad actual de alguna organización, la puesta en marcha de ésta evaluación, dio como resultado la detección de los departamentos en donde se están cometiendo más incidentes, aunque la implantación de políticas y procedimientos entorno al resguardo de datos, es una tarea difícil de cumplir ya que el personal a cargo del manejo de los sistemas lo llega a considerar tedioso e innecesario.

En los dos últimos apartados de este capítulo, se hace un estudio preliminar para conocer las necesidades reales de la organización en cuanto a la seguridad de sus bases de datos. Esto da pie a la implementación del sistema que administra la seguridad, el desarrollo de éste sistema ayuda a controlar en un 80% los accesos a las bases de datos.

En conclusión, no existe un sistema computarizado que garantice al 100% la seguridad de la información debido a la inmensa mayoría de formas con que se puede romper la seguridad de un sistema. Sin embargo una buena planeación de la estrategia para dar seguridad a la información puede resultar desde la salvación de una empresa hasta la obtención de grandes ganancias, o como ganancias indirectas mejorando la imagen y la seguridad de la empresa.

Bibliografía, Capítulo II

- ACKOFF, Russel L., "El arte de resolver problemas", Ed. Limusa, México, 1981

- A.J. Thomas I.J. Douglas "Auditoría Informática" Ed. Paraninfo, Segunda Edición

- Yann Derrien "Técnicas de la auditoría informática" Ed. Alfaomega marcombo.

- S.M. Deen "Fundamento de los sistemas de bases de datos", Colección Ciencia Informática 1985.

- E. Yourdon, "Análisis Estructurado Moderno" Ed. Prentice Hall, 1994

- Sommerville, "Software Engineering" Ed. Addison-Wesley 1996

- John G. Burch, Jr "Sistema de información teoría y práctica" Ed. Limusa 1986.

CAPÍTULO III

APLICACIÓN DEL SISTEMA DE CONTROL DE SEGURIDAD

. Objetivo:

En ésta última sección se definirá la reingeniería de software y el impacto que tiene al usarla como herramienta en la formulación del sistema global para el control de la seguridad en la organización. Además se realiza una serie de pruebas al sistema para detectar los tipos de vulnerabilidades que pueden presentarse, y la forma en como se corrigen. Así mismo se realiza un estudio de costo-beneficio para determinar la factibilidad del desarrollo del sistema. Por último, se hace un estudio de comportamiento del sistema de control de seguridad, al crecer los sistemas de información, y la información almacenada en las bases de datos.

3.1 Resultados del sistema de control de seguridad a partir de la reingeniería de software

El sistema de control de seguridad en base de datos es resultado de la visión de la corrección de anomalías sucedidas en el pasado por deficiencias en los sistemas. Estas deficiencias causaban grandes pérdidas por fugas de información en la organización.

La reestructuración de la seguridad en base de datos esta con base en la reingeniería de software, para definir lo que significó la reingeniería de software en este sistema se definirá lo que es software, su naturaleza y sus características así como la ingeniería de software:

El Software, su naturaleza y características

El SOFTWARE es:

- instrucciones
- datos

en su concepción clásica el SOFTWARE son:

programas y algoritmos + datos = programas

No obstante una definición mas elaborada podría ser: "El software son: instrucciones (programas de computadora) que cuando se ejecutan proporcionan la función y el rendimiento deseados, estructuras de datos que permiten a los programas manipular adecuadamente la información y documentos que describen la operación y el uso de los programas."[29]

Esta definición incluye: Las instrucciones que se dan al computador (programas) para que este pueda trabajar y operar. La palabra Función significa que todo programa (SOFTWARE) debe realizar algo (objetivo) o generar algo o transformar algo, generalmente son datos, pero la noción de dato e información, tiene hoy un alcance mayor, son dibujos (gráficos), sonidos, video, documentos enteros con todo lo que haya dentro del el (imágenes "escaseadas") y aun más cosas que se constituyen en información útil o de la cual se puede extraer información útil para una empresa. El SOFTWARE es un componente importante de un sistema de información, tal vez el más importante.

Un Sistema de información es: "Una disposición de componentes integrados entre si, cuyo objetivo es satisfacer las necesidades de información de una organización.

La palabra necesidad es tomada en este caso como requisito o requerimiento y es también un elemento que determina la calidad del SOFTWARE.

Los componentes mencionados en la definición se pueden agrupar en:

- personas: (usuarios, gerentes, personal técnico)
- procesos (actividades)

[29] Peter Bishop "Conceptos de Informática" Ediciones Anaya Multimedia, S.A. 1989 Capitulo I.

- datos
- Comunicación y redes
- Tecnología. (Hardware y SOFTWARE).

Analicemos ahora la Naturaleza de este producto denominado SOFTWARE:

El SOFTWARE en un producto diferente a todos los que se construyen en un procesos industriales o de ingeniería, realmente no se "fabrica" se desarrolla. A diferencia de muchos productos que se desarrollan en forma similar (análisis, diseño, construcción, pruebas) el SOFTWARE no es físico, es lógico (es abstracto) Incluso durante su construcción no es tan fácil de monitorear su grado de desarrollo debido a que no es "visible" como un puente o una máquina. Esto agrega unos niveles de complejidad a la "producción" o desarrollo de SOFTWARE.

El SOFTWARE, no se estropea por el **uso y el tiempo** sin embargo también se "deteriora" en el sentido de volverse **obsoleto**. La pregunta aquí es: ¿que hace que esto suceda?. Son varias las causales de esta situación:

- Como se requieren cambios en el SOFTWARE y mantenimiento es posible que se incluyan defectos (especialmente si esta mal diseñado). Hay SOFTWARE fácil de modificar, con estructuras adecuadas para el mantenimiento y sin incluir fallas, pero hay SOFTWARE que al contrario, cuando se hacen cambios, dejan de funcionar otras partes que desgraciadamente dependen del sitio donde se hizo el cambio. Esto es similar a que dejara de funcionar en una casa todo o gran parte del sistema eléctrico por una falla en una conexión eléctrica de una habitación.
- A diferencia del hardware y las máquinas el mal funcionamiento no se arregla cambiando una pieza o un repuesto. Por esto el mantenimiento de SOFTWARE es mas complejo que el mantenimiento de hardware.
- Las empresas, las operaciones de las empresas y los requisitos por los cuales se construyó el SOFTWARE van cambiando en el tiempo y van haciendo al software obsoleto. Se estima que un software se vuelve obsoleto en termino de **tres a siete años**, si antes un gran cambio no ocurre en cuyo caso se vuelve obsoleto en forma inmediata.
- Un cambio Tecnológico grande hace el software obsoleto. Por ejemplo, el paso de iterase DOS a Windows. EL salto de win16 a win32, La programación orientada a Objetos, la introducción de bases de datos en una Organización.
- El hecho que no se ha llegado a una industria de ensamblaje de componentes en la construcción de software (A diferencia del hardware).
- La complejidad del software es creciente.

Todos los elementos mencionados anteriormente define las características y la naturaleza de ese producto, resultado de la labor de programación, que se denomina SOFTWARE. Otra característica importante del software es que se desarrolla utilizando un lenguaje de programación con un vocabulario limitado y una gramática definida.

TESIS CON
FALLA DE ORIGEN

El desarrollo de SOFTWARE es influenciado por la evolución del hardware, el hardware se ha vuelto mas barato, mas sofisticado, más poderoso, esto ha incrementado las expectativas de lo que puedan hacer los programas que se desarrollen para estos equipos.

La complejidad en el desarrollo de software es ocasionada por dos elementos : por el tamaño y complejidad del problema y la dificultad de los usuarios para dar precisión sobre sus necesidades (requerimientos) de forma que los desarrolladores puedan comprender.

Para manejar el primer elemento, las metodologías incluyen elementos que ayudan a reducir y a manejar la complejidad de los sistemas (labor de toda la formación académica que se recibe en las Universidades e instituciones educativas), sobre le segundo elemento, además que los analistas deben tener la habilidad para "extraer" los requerimientos a los usuarios, especialmente a aquellos con dificultad para expresarlas", defiendo la teoría, de que todos los profesionales independiente de su formación, deben recibir en la Universidad un curso (o varios) donde los capaciten para definir y expresar adecuadamente requerimientos sobre sistemas, ya que con mucha probabilidad algún día tendrán que hacerlo.

El SOFTWARE, por su naturaleza, requiere de procesos de ingeniería diferentes a los de otras disciplinas. Al desarrollar software debe conocer la naturaleza del producto que se va a generar.

Ingeniería de Software

Es el término que cubre la totalidad del proceso de desarrollo (o producción) de un software. La ingeniería de software es la producción de un software profesional[30]. Incluye áreas como:

- Administración de Proyectos.
- Organización de Equipos
- Interacción Humano Máquina
- Programación, etc.

Características del producto final de la Ingeniería de Software:

- Cumplir los requerimientos del cliente.
- Tener calidad
- Estar probado
- Documentado
- Mantenido

La construcción de software debe ser una labor muy formal, que aplique modelos inclusive matemáticos para el diseño de sistemas, modelado de funciones de un negocio y modelado de los datos.

[30] Prof. Carlos A. Fernández y Fernández "Instituto de Electrónica y Computación". Universidad Tecnológica de la Mixteca (Apuntes)

TESIS CON
FALLA DE ORIGEN

La programación y el desarrollo de programas no es un arte ni tampoco una destreza que poseen algunos. Para desarrollar software existen metodologías, lenguajes y herramientas que se deben aplicar en los momentos y a los problemas que lo requieran.

La planeación y el control son elementos esenciales de todo sistema exitoso. Al desarrollar el software para el sistema, la planeación se realiza en el diseño mucho antes de que comience la programación. Se necesitamos técnicas que ayuden a poner los objetivos de los programas para que nuestros programas estén completos. También se necesitan técnicas de diseño para que ayuden a dividir el esfuerzo de programación en módulos manejables. Sin embargo, no es satisfactorio tratar de dejar las cosas simplemente en las etapas de planeación. Después de que los programas estén terminados deben recibir mantenimiento, y los esfuerzos de mantenimiento típicamente sobrepasan el esfuerzo gastado en el diseño y programación original.

Pero la metodología de análisis que se use debe de depender de:

- Tipo de software a desarrollar.
- Experiencia en la metodología.
- Lenguaje en que se va a desarrollar

Además, independientemente de la metodología de análisis, el ciclo de vida se debe elegir con base en las prioridades que se tengan.

Reingeniería de Software

La reingeniería es un proceso total de readecuación de las organizaciones a las nuevas y exigentes condiciones en un entorno cada vez más difícil de controlar; es decir, es una de las formas con que se puede operar el cambio.[31]

Esta operación de cambio, se fundamenta en las tres "C":

Cliente: el cliente es la razón de ser del servicio, es a quien buscamos satisfacer y por lo tanto hay que pensar cómo él desea ser atendido.

Competencia: Las organizaciones deben ser cada vez más competitivas, para así poder sobrevivir en un entorno cambiante y exigente en aras de tener y preservar su segmento de mercado.

Cambio: Busca que las Empresas sean más efectivas. Eficiencia + eficacia = efectividad

[31] Díaz Gustavo. "Como operar el cambio vía reingeniería". Revista Acta Académica. Universidad Autónoma de Centro América. número 22. Mayo 1998

TESIS CON
FALLA DE ORIGEN

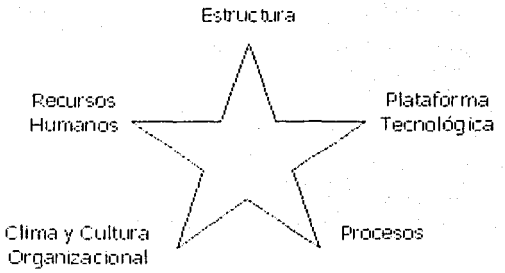


Figura 3.1 Cinco campos sustanciales en los que actúa la reingeniería.

Estructura

Se deben eliminar en las organizaciones las estructuras piramidales, ya que éstas producen lentitud, centralización, inflexibilidad y protección a los trabajadores ineficientes e ineficaces; claro está, debemos estructurar en forma más vertical; descentralizando así las decisiones y facilitando la comunicación. Debemos organizarnos de afuera hacia adentro, pensando siempre en el cliente.

Se debe eliminar el concepto de jefe, y cambiarlo por el de proveedor de información y soluciones; además, tomar en cuenta que los recursos humanos ya no se administran, sino más bien se lideran. Se reconoce también que ahora el trabajador se evalúa no sólo por su coordinador inmediato sino también por sus compañeros, clientes y colaboradores.

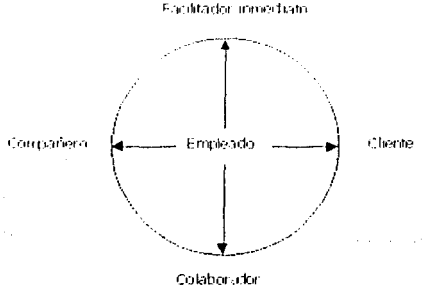


Fig. 3.2 Estructura ideal de la interrelación del empleado

TESIS CON
FALLA DE ORIGEN

Procesos

El trabajo se debe organizar por sistemas básicos y de ahí, segregar los procesos y subprocesos; tenemos por ejemplo los sistemas básicos:

- Técnico
- Táctico
- Estratégico
- Administrativo

Debe haber un enfoque sistémico: todo hacia el cliente.
Las jefaturas se deben estructurar por procesos, para evitar los obstáculos en cada uno de ellos.
La responsabilidad debe ser por resultados, sin excusas.

Tecnología

La tecnología debe estar al servicio del cliente; a través de ella se hace un mejoramiento de la capacidad decisoria del personal. La tecnología facilita el diseño de los sistemas de información para la calidad del servicio, siempre pensando en el cliente. Así se debe manejar más información y menos papeles.

Clima y cultura organizacional

Los valores de los trabajadores y la organización, deben ser compartidos, creando un clima propicio para la iniciativa, el aporte y el reconocimiento. Los estilos gerenciales deben ser comunicativos y participativos, creadores de compromiso, entrega, entusiasmo y compromiso grupal intenso. Todos los trabajadores deben ir tras lo mismo: Misión / Visión

Recursos Humanos

El primer punto que toca la reingeniería de Recursos Humanos, es la polifuncionalidad del personal y la rotación de puestos. Todos los trabajadores saben hacer todas las tareas de todos los puestos de la organización. Las funciones del personal deben ser enriquecidas con tareas que saquen el puesto de la rutina y, por supuesto, que lleven al trabajo en equipo.

Además, ya se elimina el concepto de "Manual de Puestos" cambiándolo por "Manual de Clases", es decir, las clases ya no deben ser estrechas sino más anchas. En los recursos humanos de la organización se debe inculcar el sentido de pertenencia, orgullo y solidaridad laboral. Se debe eliminar la concepción de los trabajadores de que el trabajo es un castigo divino, cuando más bien es fuente de retos y satisfacciones.

Los recursos humanos podrán enfrentarse al futuro competitivo sólo a partir de una adecuada capacitación, dirigida siempre a enfrentar necesidades reales y de acuerdo con los planes estratégicos de la empresa. Además, se debe tener una visión de largo plazo en la contratación; de nada podrá servir a los empresarios la rotación de personal en caso contrario, pues no podrán capitalizar el recurso humano.

TESIS CON
FALLA DE ORIGEN

De lo anterior se desprende que las organizaciones, como entes dinámicos que son, necesitan brindar una efectiva respuesta a las demandas de un entorno cambiante y cada vez más exigente; además, tenemos que poner especial atención a los planos organizativo dinámico, estructural y funcional, lo que permitirá un análisis integral de la organización para poder operar este cambio vía de la reingeniería.

Antes de iniciar el cambio como tal, debemos hacer un diagnóstico organizativo de la situación, pues operar el cambio ya sea por vía de la Reingeniería, Calidad Total, Círculos de Calidad o cualquier otro tipo de operación del cambio, requiere un análisis de la organización y su entorno.

Reingeniería del sistema de control de seguridad en base de datos de la organización

Comparación del ciclo de vida de los sistemas anteriores con el sistema de control de seguridad

La idea de reestructurar la seguridad en la base de datos, se debe a constantes reclamos de los usuarios de sistemas, al no tener accesos a cierta información, necesaria para realizar sus actividades y el tiempo que lleva reasignar sus accesos, o inconsistencia de información en la base de datos, por no tener bien administrados los permisos de los sistemas. Esto va en aumento, dependiendo de la cantidad de usuarios en la organización. Dado este problema, se investigó el ciclo de vida del software desarrollado en la empresa de estudio, hasta el momento. Este ciclo de vida se muestra en la siguiente gráfica:

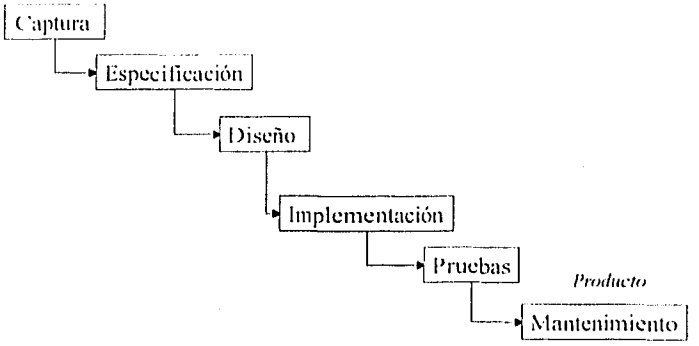


Fig. 3.3 Método cascada del ciclo de vida de los sistemas usado en la organización de estudio

La característica principal del método del ciclo de vida, es que no se puede regresar a ninguno de los puntos anteriores, una vez desarrollados. Esto trajo consigo deficiencias en los sistemas desarrollados, ya que sino estaba bien desarrollada la especificación ocurría una serie de problemas una vez concluidos.

TESIS CON
FALLA DE ORIGEN

Uno de éstos problemas es el control de la seguridad y auditoría del software de base de datos desarrollados hasta el momento. El problema comenzó a tomar importancia cuando la información en la base de datos aumentaba, así como los usuarios de los sistemas.

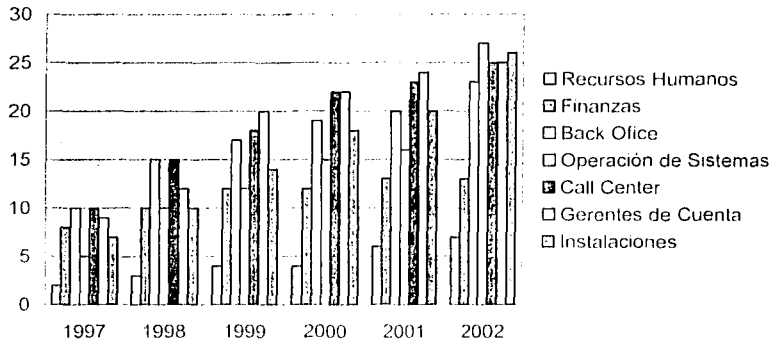


Fig. 3.4 Relación de crecimiento de usuarios, dividido por departamentos en la organización de estudio.

El ciclo de vida de software usado para el desarrollo del sistema de control de seguridad es el método de cascada con retorno, mostrado en la siguiente figura:

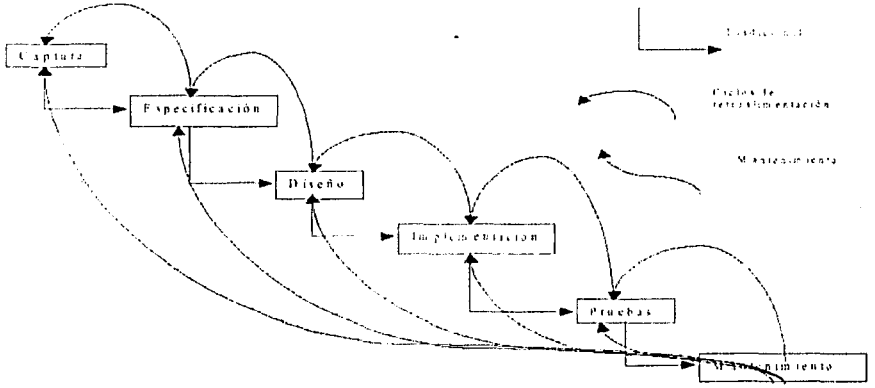


Fig. 3.5 Método cascada con retorno, del ciclo de vida del sistema de control de seguridad

TESIS CON
FALLA DE ORIGEN

En el peor de los casos, el cliente no se da cuenta de que su sistema se esta construyendo de forma errónea hasta que el software se libera. Por eso, el método de cascada con retorno se debe de realizar en cada etapa la verificación y validación, y el resultado será utilizado dentro del proceso de desarrollo[32]

Comparación en la asignación de sistemas respecto al método anterior con el sistema de control de seguridad

Los siguientes pasos, es la forma en como técnicamente se crea un nuevo perfil de acceso con el sistema manejador de base de datos (Data Base Magnament System. DBMS) ORACLE.

Crear un Nuevo Perfil con el sistema anterior (Forms 6.0 y PL/SQL)

1.- Sobre la base de datos de producción dar la siguiente instrucción:

```
CREATE ROLE nombre_perfil;
```

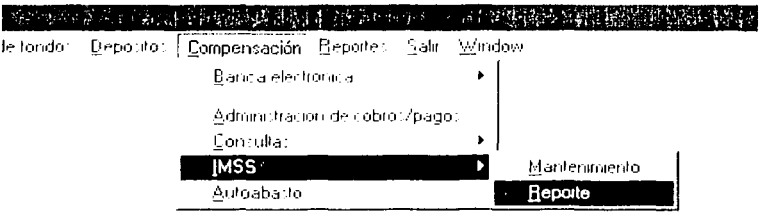
2.- Asignar privilegios de acceso y transacciones sobre los objetos de bases de datos (tablas, vistas, secuencias, procedimientos, funciones paquetes) de determinada aplicación a el perfil, por ejemplo:

```
                    COMPENSACION
                        IMSS
              IMSS MNTO
GRANT SELECT ON REG_ESTABLECIMIENTOS_CONTROL TO nombre_perfil;
GRANT UPDATE ON REG_ESTABLECIMIENTOS_CONTROL TO nombre_perfil;
GRANT INSERT ON REG_ESTABLECIMIENTOS_CONTROL TO nombre_perfil;
GRANT DELETE ON REG_ESTABLECIMIENTOS_CONTROL TO nombre_perfil;
GRANT SELECT ON CAT_ESTABLECIMIENTOS TO nombre_perfil;
          IMSS REPORTE
GRANT SELECT ON REG_TRANSACCIONES TO nombre_perfil;
GRANT SELECT ON CAT_ESTABLECIMIENTOS TO nombre_perfil;
GRANT SELECT ON CAT_CLIENTES TO nombre_perfil;
GRANT SELECT ON CAT_BANCOS TO nombre_perfil;
GRANT SELECT ON CAT_CUENTAS_ESTABLECIMIENTOS TO nombre_perfil;
GRANT SELECT ON REG_ESTABLECIMIENTOS_CONTROL TO nombre_perfil;
          REPORTE: IMSS DIARIO
    GRANT SELECT ON REG_TRANSACCIONES TO nombre_perfil;
    GRANT SELECT ON CAT_ESTABLECIMIENTOS TO nombre_perfil;
    GRANT SELECT ON CAT_CLIENTES TO nombre_perfil;
    GRANT SELECT ON CAT_BANCOS TO nombre_perfil;
    GRANT SELECT ON CAT_CUENTAS_ESTABLECIMIENTOS TO nombre_perfil;
    GRANT SELECT ON REG_ESTABLECIMIENTOS_CONTROL TO nombre_perfil;
          REPORTE: IMSS SEMANAL
    GRANT SELECT ON REG_TRANSACCIONES TO nombre_rol;
    GRANT SELECT ON CAT_ESTABLECIMIENTOS TO nombre_rol;
    GRANT SELECT ON CAT_BANCOS TO nombre_rol;
```

[32] Prof. Carlos A. Fernández y Fernández. Instituto de Electrónica y Computación. Universidad Tecnológica de la Mixteca

TESIS CON
FALLA DE ORIGEN

Esta es la forma en como esta estructurado actualmente el archivo de perfiles. Notar que "*COMPENSACION*" corresponde al nombre del módulo en el menú de la "Aplicación de clientes oracle".



3.6 Menú usado para el llamado de aplicaciones

"*IMSS*" corresponde al submenú del módulo.

"*IMSS MANT*" Corresponde a los privilegios que utiliza la aplicación de Mantenimiento. Se puede apreciar en el archivo que las líneas punteadas son de menor longitud que el submenú de "*IMSS*"

"*IMSS REPORTE*" Corresponde a los privilegios que utiliza la aplicación de Reporte. Se puede apreciar que las líneas punteadas son de menor longitud que el submenú de "*IMSS*"

"*IMSS DIARIO*" Son los objetos usados por el reporte "IMSS DIARIO" que es llamado mediante la aplicación de "Reporte". Se nota en el archivo de roles que la tabulación con respecto a la aplicación de "Reporte" es mayor, esto indica que trata de asignación de privilegios sobre un reporte.

"*IMSS SEMANAL*" Son los objetos usados por el reporte "IMSS SEMANAL" que es llamado mediante la aplicación de "Reporte". Se nota en el archivo de roles que la tabulación con respecto a la aplicación de "Reporte" es mayor, esto indica que trata de asignación de privilegios sobre un reporte.

3.- Conectarse con el usuario SYSTEM y con el password MANAGER sobre la base de datos de ORACLE y asignar el siguiente privilegio:

GRANT SELECT ON FRM50_ENABLED_ROLES TO *nombre_perfil*;

TESIS CON
FALLA DE ORIGEN

4.- En Forms 6.0[11] abrir el menú usado por la aplicación de oracle (MENUMAIN). Dar de alta el perfil o role en las propiedades del "Menu Module", en la propiedad "Module roles":

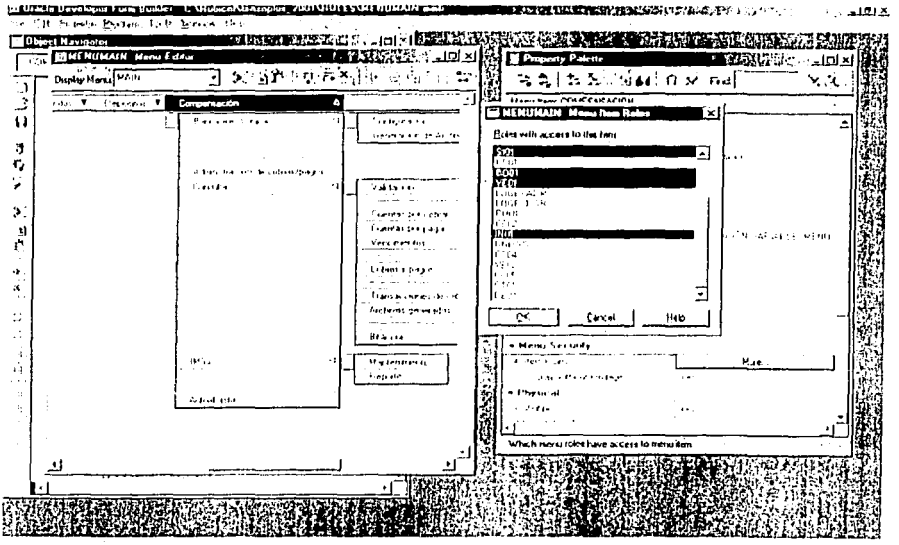


Fig. 3.7 Asignacion de aplicaciones por medio de la herramienta de desarrollo de ORACLE (Forms)

Hacer lo mismo para las propiedades de cada submenú y para cada aplicación del menú asociando el nuevo role.

5.- Compilar el archivo "MENUMAIN", se generará el archivo ejecutable MENUMAIN.mmx y copiarlo en la siguiente ruta:

SRV_TELEFONELL\SOFTWARE\FACTURACION

Crear un nuevo perfil con el sistema de control de accesos a la base de datos

1.- En la barra de tareas del sistema de control de accesos oprimir el botón "Editar Menú"

[11] Forms 6.0 es una aplicación de ORACLE tipo "Aplicación de usuarios" que sirve para desarrollar pantallas menús y librerías de base de datos

TESIS CON
FALLA DE ORIGEN

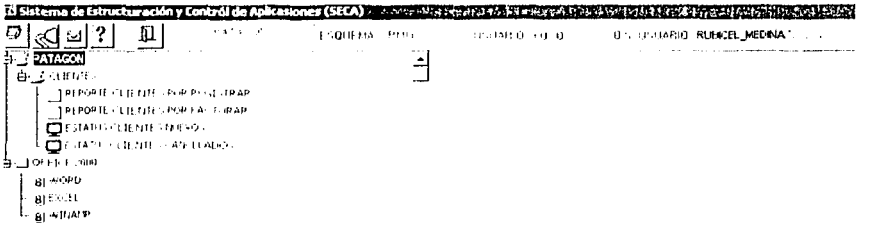


Fig. 3.8 Pantalla principal del sistema de control de accesos.

2.- Se desplegará la siguiente venta de opciones, seleccionar la opción "Crear Role" y oprimir el botón aceptar.

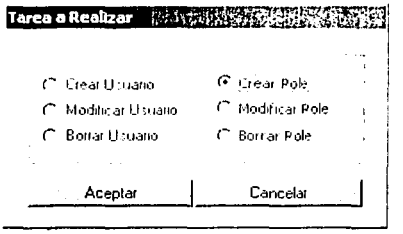


Fig. 3.9 Ventana de tareas a realizar del sistema de control de accesos a la base de datos.

3.- Al dar aceptar en la ventana anterior, se desplegará la siguiente ventana. En este punto, se debe de indicar el nombre del perfil o role a crear.

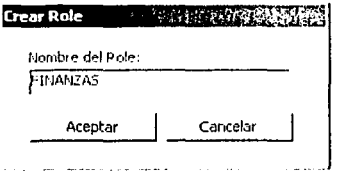


Fig. 3.10 Ventana del nombre del role o perfil a crear

4.- Al ingresar el nombre del nuevo perfil, y oprimir el botón aceptar, se creará un nuevo role de base de datos, y quedará listo para ser editado, con la siguiente ventana, que se desplegará automáticamente.

TESIS CON
FALLA DE ORIGEN

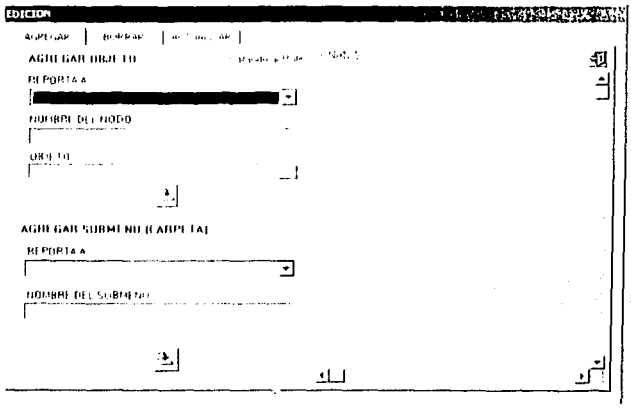


Fig. 3.11 Ventana de edicion de aplicaciones asignadas al nuevo roele o perfil de acceso

5.- En la opción "Agregar Submenú" se debe de indicar el nombre del módulo o submodulo que se pretende crear. Al dar el botón aceptar, en la parte derecha de esa ventana se visualizará como se va formando el menú del perfil o role.

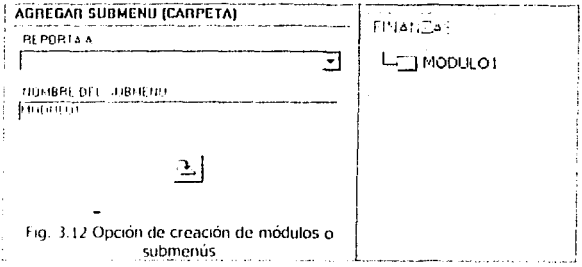


Fig. 3.12 Opción de creación de módulos o submenús

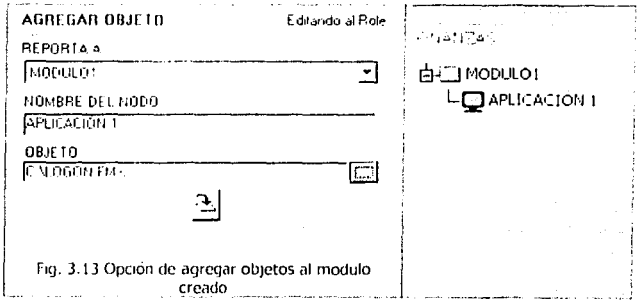


Fig. 3.13 Opción de agregar objetos al modulo creado

Nota: Los permisos sobre los objetos asignados a la aplicación que se pondrá en el menú, se dan de alta en una pantalla de tipo catálogo.

Los pasos antes descritos, se deben de realizar para aplicación que se desea asignar al perfil.

En el caso de la implementación del sistema de control de seguridad en base de datos, implico cambiar la cultura tanto de los programadores y gerentes de sistemas como de los usuarios y del ambiente en el cuál estaban acostumbrados a trabajar. La operación al cambio se implementa de la siguiente manera:

Al cliente (usuarios de los sistemas) se le explico las ventajas que implicaba la implementación de este sistema por el anterior, ya que ahora podía tener control de aplicaciones tanto de los sistemas de la empresa (Sistemas de Bases de Datos desarrollados con Developer/2000), como de aplicaciones propias del sistema operativo Windows (Windows 95, 98, 2000), en un solo menú, además de poder mandar correo electrónico (con base en Microsoft Outlook), editar su menú y reconectarse a los sistemas de base de datos todo, en usa sola aplicación.

Esto convenció al cliente de cierta forma a cambiarse a este nuevo sistema de control de seguridad en base de datos y adaptarse a los estándares para su uso.

Además a los gerentes de la organización se les hizo ver que el cambio a este sistema de control de seguridad podía tener mayor ventaja en cuanto a que se puede saber quien y a que hora hizo cada una de las transacciones correspondientes a los sistemas de la empresa, además la forma en como se restringen los accesos y la forma amigable en la cual se pueden mover los parámetros del sistema para cambiar los criterios de conexión.

El cambio de estructura en los sistemas de la organización significa hacer una reingeniería en el software, causando con esto un esfuerzo de todas las partes que componen la organización, pero esto se traduce en puntos clave para el éxito de la organización y estar en ventaja ante la competencia al tener completo control sobre la información almacenada en las bases de datos.

Esquema global para el control de la Seguridad en las Bases de Datos

El plan de trabajo que contempla la planeación del control de la seguridad en la información de la base de datos (ORACLE), toma en cuenta la realización de actividades en dos (2) etapas sucesivas:

Relevantamiento y Diseño: Infraestructura de Tecnología (IT) y Arquitectura de Seguridad

Descripción de las actividades:
Esta etapa tiene como objetivo comprender las características operativas y de administración de la infraestructura informática de la organización enfocadas a las base de datos, la política y los procedimientos de seguridad informática en uso y detectar requerimientos de seguridad implícitos no contemplados.

A fin de alcanzar los objetivos propuestos se realizarán varias reuniones con personal clave de la organización relacionado con el proyecto y se requerirá toda la documentación existente

TESIS CON
FALLA DE ORIGEN

relacionada con la infraestructura de tecnología y la seguridad informática de la organización. Para el proyecto de servicios en línea, se determinará la topología de red, plataformas, servicios internos y públicos que se brindan, aplicaciones propietarias y de terceros, el uso general de la infraestructura de tecnología y su relación con los negocios de la organización.

Esto permitirá detectar los expuestos de seguridad teóricos en el esquema e identificar los requerimientos mínimos a cubrir para los conceptos de autenticidad de las transacciones, integridad de datos, disponibilidad de la infraestructura, refutabilidad de las transacciones y confidencialidad de los datos.

Los datos relevados se formalizarán en un modelo de amenazas y atacantes que identifique y cuantifique el riesgo de seguridad, el impacto de la explotación de los problemas detectados y caracterice a potenciales atacantes, clasificándolos en función de su perfil y los recursos de los que disponen. Se diseñará y documentará una arquitectura de seguridad que contemple las necesidades y requerimientos detectados y que proteja efectivamente de ataques y vulnerabilidades descritas en el modelo de amenazas y atacantes elaborado.

Para la realización de las actividades contempladas en esta etapa se requerirá de la organización la provisión de la documentación de diseño, especificaciones técnicas, manuales de procedimientos y operaciones de los componentes de la infraestructura de I.T.
Así mismo, se requerirá la documentación existente correspondiente a política y procedimientos de seguridad informática de la organización.

Una vez elaborando el plan anteriormente descrito, se implementará la arquitectura de la seguridad, tomando como apoyo la auditoría de los sistemas. Para hacer esto se utilizará la información relevada en la primera etapa se realizará una auditoría de todos los componentes de la infraestructura de tecnología contempladas en la sección "Alcance" de esta descripción.

Se pone especial énfasis en verificar la existencia de contramedidas para todos los problemas descriptos en el documento "Modelo de amenazas y atacantes" y se identificarán problemas específicos de implementación y configuración en todos los componentes de la infraestructura, así como contravenciones de la política y procedimientos de seguridad informática explicitados en "Modelo de amenazas y atacantes".

Las actividades de esta etapa comprenden la realización de una prueba de intrusión asumiendo un perfil de atacante externo, a fin de identificar vulnerabilidades y fallas en la implementación de la arquitectura de seguridad. Como resultado de esta etapa se dispondrá de información precisa sobre los expuestos de seguridad prácticos en la implementación de la arquitectura de seguridad de la organización, y recomendaciones especificas para la solución en el corto plazo de los problemas detectados.

No están dentro del alcance de la implementación del control de seguridad:

- Mecanismos y medidas de seguridad de organizaciones relacionadas con el cliente, proveedores de tecnología, conectividad o servicios para la infraestructura de IT.
- Sistemas y componentes de la infraestructura de tecnología de la organización que no tiene relación directa.

TESIS CON
FALLA DE ORIGEN

Diseño de la arquitectura de seguridad

La seguridad debe ser contemplada en varios niveles de la organización, para tener una control en cuanto a los accesos de la información en la base de datos, se debe de empezar desde la administración de la red. Generalmente en las organizaciones, el área que lleva éstas tareas, es el área de "Redes y Soporte Técnico".

El área de "Redes y Soporte Técnico" lleva el control de los accesos en la red y asigna niveles de seguridad sobre los usuarios del sistema operativo, en éste caso el sistema operativo es Windows NT. Otros servicios que presta el área es soporte a:

- Correo interno y externo
- Acceso a internet
- RAS (Servicio de acceso remoto)
- Servidor de Fax
- Respaldos de la información en la base de datos.

Esta área debe de interactuar estrechamente con el administrador de la base de datos (DBA), para que el administrador, conozca la potencialidad que le puede ofrecer la red y que ventajas a puede implantar al trabajar en un ambiente Cliente-Servidor[34],

El papel del Administrador de base de datos como se observó en el capítulo I, es:

- Entender la arquitectura de los manejadores de bases de datos utilizados en la organización.
- Garantizar el correcto funcionamiento de las bases de datos.
- Definir estrategias de manejo de los discos.
- Diseñar el sistema de backups de la base de datos.
- Dimensionar las bases de datos y crear la base de datos.
- Afinar la base de datos, optimizando su desempeño y tiempo de respuesta.
- Instalar nuevas versiones de los manejadores de bases de datos que posee la institución.
- Asesorar a los analistas en el diseño del modelo de datos de cada sistema de información.
- Cuidar la integridad del modelo de datos corporativo.

Con la implementación del sistema de control de seguridad en base de datos, el administrador de la base ya no realizará las siguientes actividades, que comúnmente formaba parte de sus tareas diarias:

- Definir perfiles de usuario, otorgar privilegios, matricular usuarios.
- Establecer mecanismos para garantizar la seguridad de los datos almacenados en la base de datos.

El área de "Operación de Sistemas", tiene a cargo las siguientes tareas:

[34] El ambiente Cliente-Servidor es la forma en como operan los sistemas manejadores de bases de datos

TESIS CON
FALLA DE ORIGEN

- Validación de procesos de carga de información a la base de datos
- Monitoreo de procesos realizados automáticamente
- Recibe las anomalías o la inconsistencia de información detectadas por el departamento de "Conciliación de información y auditoría de sistema".
- Pone en producción nuevos sistemas, liberados por el departamento de "Control de calidad de los sistemas"
- Asigna permisos de transacciones sobre la información, para los "Gerentes de área", a través del sistema de control de seguridad en bases de datos.
- Establece mecanismos para garantizar la seguridad de los datos almacenados en la base de datos. (tarea, anteriormente realizada por el DBA).

El departamento de "Diseño y Desarrollo de Sistemas", busca analizar sistemáticamente la entrada de datos, el proceso o transformación de los datos, el almacenamiento de datos y la salida de la información dentro del contexto del negocio.[15]

Para lograr el objetivo del área, se deben de elaborar los diseños funcionales y técnicos de los sistemas a desarrollar, así como desarrollar procesos, e interfaces finales, para la manipulación de la información almacenada en la base de datos.
Una vez terminado el desarrollo de un nuevo sistema, interfaz o proceso, es pasado al área de "Control de Calidad en los sistemas" para su evaluación. Si el departamento de calidad reprueba el sistema, lo recrea al departamento de "Diseño y Desarrollo de Sistemas", para hacer las correcciones o cambios correspondientes.

El área de "Control de calidad en los sistemas" se encarga de evaluar todos los programas de aplicación recientemente escritos o modificados de un sistema, así como los nuevos manuales de procedimientos.

Este departamento debe probar al sistema trabajando como un todo. Esto incluye probar las interfaces entre subsistemas, la corrección de la salida y la utilidad y comprensibilidad de la documentación de la salida del sistema.

Cualquier inconsistencia en los sistemas desarrollados, se regresarán al departamento de "Diseño y Desarrollo de Sistemas", para que los corrijan a lo antes posible. Una vez aprobado el programa, interfaz o manual de procedimiento, se le indicará al departamento de "Diseño y Desarrollo de Sistemas" para que lo ponga en producción.

El departamento de "Conciliación de información y auditoría de sistemas" se encarga de asegurar la confiabilidad de la información en la base de datos, ésta tarea la realiza apoyándose con documentación emitida por entidades externas a la organización (bancos, organizaciones afiliadas al negocio, etc.), por ejemplo, estados de cuenta, facturas, reportes de tipo fiscal, etc.

Además, dicho departamento, estudia los controles usados en el sistema de información para asegurarse de que sean adecuados y que estén haciendo lo que se pretende que hagan. Esta tarea la realizan tomando como herramienta el "Sistema de control de seguridad en bases de datos", en el módulo de "Auditoría de transacciones".

[15] Kendall & Kendall , Análisis y Diseño de Sistemas Prentice Hall Hispanoamericana, S.A. de C.V. 1997

TESIS CON
FALLA DE ORIGEN

Cualquier falla de consistencia de datos, o detecciones de fraudes, el personal del departamento de "Conciliación de información y auditoría de sistemas" debe de registrarlo en el mismo sistema de "Sistema de control de seguridad en bases de datos", en el módulo de "Detección de Inconsistencias de Información".

La información registrada, además de ser detallada en el rubro del sistema, debe de ser informado al departamento correspondiente, para que el problema sea atendido de forma inmediata.

La manera en como se escalarán los problemas detectados por el área de "Conciliación de información y auditoría de sistemas" , se muestra en la siguiente gráfica:

Fig. 3.11 Escalamiento de responsabilidades [36]

En resumen, las funciones del departamento de "Conciliación de información y auditoría de sistemas" es:

- Participar en el desarrollo del modelo de seguridad informática de la Dirección.
- Contribuir al desarrollo del modelo de aseguramiento de la calidad de los sistemas informáticos.
- Participar en la formulación y actualización del plan de contingencia.
- Participar en el desarrollo e implantación de políticas de seguridad informática.
- Colaborar en la formulación y evaluación del plan periódico de auditorías informáticas.
- Participar en el desarrollo de metodologías de auditoría informática y aplicarlas.
- Programar y ejecutar auditorías a unidades y sistemas informáticos.

[36] Pirámide de escalamiento de responsabilidades a seguir al encontrar incidentes en la información de la base de datos

TESIS CON
FALLA DE ORIGEN

- Realizar las actividades de seguridad requeridas en cada una de las fases del ciclo de vida de los sistemas informáticos.
- Monitorear y evaluar el cumplimiento y aplicación de políticas, normas, estándares y procedimientos informáticos; Sugerir los ajustes requeridos en función de cautelar los intereses de la Dirección.
- Hacer cumplir las políticas, normas y procedimientos informáticos.
- Revisar y evaluar las medidas de seguridad de acceso físico, consulta y niveles de utilización de datos y aplicaciones.
- Vigilar el cumplimiento de metodologías adoptadas por la Dirección.
- Participar en el desarrollo de sistemas de información y sugerir la incorporación de las medidas de seguridad requeridas.
- Inspeccionar la operación de sistemas en producción.
- Investigar la causa de los problemas surgidos en la operación de los sistemas y proponer correctivos.
- Evaluar integralmente las aplicaciones desarrolladas y los software aplicativos adquiridos.
- Evaluar el diseño, operación, seguridades, integridad y manejo de las bases de datos.
- Realizar pruebas para verificar la seguridad de los recursos de la red de la Dirección.
- Inspeccionar la operación del hardware y comprobar la existencia y aplicación de prácticas de respaldo y de control de datos almacenados.
- Participar en la evaluación de la ejecución del plan de sistemas informáticos y de los planes operativos de la Dirección.
- Cumplir con las normas, reglamentos y procedimientos establecidos por la Dirección y por el MEYF para el desarrollo de las funciones asignadas.
- Las demás funciones que le asigne su superior inmediato y que guarden relación con la naturaleza de su cargo.

Las responsabilidades del departamento, son:

- Responde por la ejecución de auditorías informáticas.
- Cuida de la seguridad informática en el desarrollo de sistemas de información.
- Desarrolla metodologías de auditoría informática.
- Evalúa políticas, normas y procedimientos informáticos.
- Inspecciona y evalúa bases de datos y sistemas en producción.
- Realiza pruebas para comprobar la integridad de los datos o información de la Dirección.
- Elabora informes de auditoría de sistemas

El "Gerente de Área" se dedica a dirigir los planes operativos del departamento que tiene a su cargo, además de poner en practica toda esta nueva filosofía implantada por la organización.

Con el "Sistema de Control de Seguridad en Bases de Datos", el gerente asignará los accesos de los sistemas a sus subordinados, dependiendo de las funciones de cada uno de los integrantes del área, y él será el responsable de tomar decisiones de quienes podrán hacer transacciones o consultas de la información a la base de datos.

Al implantar "Sistema de Control de Seguridad en Bases de Datos", en la organización, y legarle la responsabilidad de accesos y transacciones de la información de las bases de datos a nivel gerencia, se logrará una nueva cultura de negocio, en la que el empleado entiende cómo es un proceso horizontal, busca hacer más eficiente su trabajo con información integrada, y se enfoca a la rentabilidad del negocio, que significa una buena relación con el cliente, productividad, innovación, creatividad y buenos resultados.

Procedimiento de Control de Cambios

Para el caso de los cambios en programas o utilitarios se seguirá el siguiente procedimiento.

-Recepción del requerimiento por parte del usuario autorizado.

- Evaluación del impacto a causarse con el cambio.

- Aprobación de usuario de los riesgos e impacto a causarse con el cambio.

- Ejecución del cambio en ambiente de desarrollo.

- Definición de pruebas del cambio solicitado.

- Pruebas del cambio por personal de desarrollo en ambiente de desarrollo.

- Auditoría de sistemas al cambio a realizarse.

- Control Interno del cambio a realizarse.

- Depuración del cambio luego de auditoría y control interno.

- Pruebas del cambio por parte de los usuarios, en ambiente de desarrollo.

-Aprobación formal del Usuario en el registro de control de cambios.

- Aprobación formal del Responsable de Sistemas en el registro de control de cambios.

-Determinación de Instrucciones y criterios por escrito, necesarios para la correcta transferencia al ambiente de producción y su reversión en caso de que sea necesario ejecutarlo.

-Determinación de lugar, fecha, hora, recursos físicos y humanos requeridos para la implementación del cambio en el ambiente de producción.

TESIS CON
FALLA DE ORIGEN

Procedimientos de la función de Producción y Operaciones.

Para el caso de la organización del área de producción y operaciones se contemplará lo siguiente:

- El personal de operación no deberá desempeñar ningún rol en la creación o modificación de programas o aplicaciones o de sistemas.

- No deberá tener responsabilidades de actualización del sistema operativo.

- No deberá tener acceso como usuario a aplicaciones específicas.

-Deben tener una descripción del cargo y funciones específicas y ser adecuadamente entrenado para cumplir con sus responsabilidades.

-Deberá contar con adecuada supervisión para asegurar el correcto cumplimiento de sus deberes.

Para el caso de la Planeación y seguimiento de la producción se contemplará lo siguiente:

-Solo las tareas autorizadas serán procesadas con datos de producción, minimizando así el riesgo de omisión y con un orden y planificación predecible.

-Es preferible que las actividades de planeación de carga, ejecución y seguimiento de procesos sean lo mas automatizado posible.

-En casos de que la intervención del operador sea inevitable, deben entregarse instrucciones precisas para las actividades a realizar, las cuales deben ser registradas y analizadas posteriormente.

-En caso de resultados emergentes, se deberá contar con procedimientos de contingencia para dar respuesta a dichos resultados.

-La planeación de los procesos debe considerar la prioridad de este entre las diferentes aplicaciones.

-Deben implantarse controles para prevenir o detectar la ejecución de tareas no autorizadas por la planeación de la producción.

-Para los casos en que usuarios requieran de tareas no establecidas o incluidas dentro de la planeación de la producción, se debe establecer un procedimiento de excepción adecuadamente controlado y con las autorizaciones correspondientes.

-El ambiente de producción y los procedimientos de operaciones deberán garantizar que sea utilizada la versión correcta de programas y los archivos respectivos.

Para el caso de la documentación se contemplará lo siguiente:

TESIS CON
FALLA DE ORIGEN

- Una planeación o cartilla diaria, paso a paso de las actividades normales del operador.

- Una planeación o cartilla diaria de los procesos con inicio y fin de cada operación.

- Los procedimientos de contingencia para los procesos

- Los procedimientos de contingencia para las fallas de hardware, software, telecomunicaciones.

- Las instrucciones en el manejo de medios magnéticos y registros de aquellos que ingresan o son retirados de la sala.

- El registro de problemas del área de operaciones

- El registro de accesos a la sala de computación.

- El responsable del área de sistemas debe asegurar que toda la documentación requerida para las operaciones esté completa, correcta y actualizada.

Para el caso de la administración de problemas se contemplará lo siguiente:

-Todas las fallas operacionales e incidentes anormales, deberían ser registrados en un Reporte de Problemas, con los detalles de hora, tipo de problema, síntomas y las acciones iniciales realizadas. Cada reporte deberá ser identificado en forma única y se deberá asignar lo más rápidamente posible la responsabilidad para su investigación y resolución.

-Mantener un registro de los problemas el cual deberá ser revisado periódicamente por el Responsable de sistemas.

-Todas las llamadas que requieran el soporte de proveedores o personal de sistemas, deben ser registradas con información del tiempo de respuesta de tales llamadas y las acciones tomadas, para su análisis posterior.

-Debe existir un procedimiento de revisión regular que incluya un análisis de tendencia de los problemas y permita asegurar que todos son resueltos.

-Se debería considerar la evidencia registrada en el sistema de administración de problemas, a objeto de tomar decisiones relativas a la oportunidad que se realice el mantenimiento de rutina y reemplazo de equipamiento.

-Todas las soluciones identificadas como cambios a ser incorporadas en el ambiente de producción, deberán ser registradas, seguidas y manejadas por los procedimientos de control de cambio. Adicionalmente se deberá registrar el origen de la solución, identificando cual fue el problema o falla.

-Informar a todos los usuarios afectados por el impacto de los problemas identificados y de los progresos obtenidos en la solución del problema

TESIS CON
FALLA DE ORIGEN

Políticas Administrativas

Vacaciones

El personal que deba tomar vacaciones y principalmente del área de sistemas de la empresa, lo realizará conforme a las disposiciones internas. Se sugiere que dicho personal no haya dejado de tomar por propia voluntad sus vacaciones por un periodo de 2 años. Algunos fraudes informáticos tienden a descubrirse cuando quienes los cometen toman vacaciones; tiempo en el cual no tienen acceso al sistema o son reemplazados mientras duran sus vacaciones. Cabe indicar al Administrador de Empresas que este es un punto de seguridad básica que debe tomar muy en cuenta dentro de los controles administrativos.

Entrenamiento

El personal de sistemas debe acogerse al plan de entrenamiento que la empresa tenga, siguiendo los estándares y procedimientos de seguridad de datos y a los aspectos específicos de seguridad de su puesto de trabajo.

Uso de Recursos Computacionales

El uso de recursos computacionales para asuntos personales debe quedar prohibido.

El software que cada usuario opere debe ser asignado de acuerdo a su utilización y el cual debe constar con las licencias respectivas. Los empleados deben estar familiarizados con el almacenamiento de datos de carácter sensitivo o confidencial.

Cabe indicar que cada usuario es responsable por el equipo asignado, software utilizado, datos contenidos en él y utilitarios que opere. La empresa debe establecer políticas y reglamentos claros respecto del uso de software ilegal (sin licencia) y los no correspondientes a los estándares de la empresa. De igual forma la empresa debe establecer un uso y propiedad claramente establecidas sobre los programas elaborados o desarrollados por personal interno, lo cual normalmente se deja reglamentado dentro de los contratos de trabajo.

Recomendaciones en torno a cambio y reingeniería en el sistema de control de seguridad

El implementar el sistema de control de seguridad en base de datos la organización requiere, al menos, cuatro etapas según Paul Hersey y Kenneth Blanchard[37]

- Conocimiento de lo que se quiere cambiar.
- Internacionalización de lo aprendido.
- Cambio en el comportamiento organizacional.
- Cambio grupal.

[37] Hersey, Paul. "Estilo Eficaz De Dirigir - Liderazgo Situacional, No Existen Dos Situaciones Iguales". Paul Hersey Y Ken H. Blanchard. Mexico, D.F. - Idh Ediciones, C1981.

TESIS CON
FALLA DE ORIGEN

Es necesario el diseño de una metodología para la implementación del sistema de operación que elimine o, al menos, minimice, la resistencia al cambio en el personal operativo del sistema, a través de:

- Diagnóstico o encuesta de actitud dirigida al personal.
- Definición de una estrategia para la sensibilización, concientización y dotación de conocimientos sobre reingeniería, poniendo énfasis en información sobre mecanismos y sus beneficios.
- Determinar los sistemas básicos de la organización: estratégico, táctico, técnico y administrativo, claro está, en una forma participativa.
- Formulación de una nueva Misión / Visión.
- Identificación de Macroprocesos y subprocesos dentro de la estructura.
- Ejecución de actividades dirigidas a todo el personal, a modo de presentación y justificación de los cambios, a título preliminar, siempre a título de recomendación y que permita, por supuesto, sugerencias de los trabajadores.
- Acercamiento práctico a la realidad; aquí podemos hacer una simulación con una prueba para analizar la respuesta.
- Una implantación definitiva exclusivamente cuando se esté seguro de la funcionalidad de la operación.
- Cultura de la operación que se adopte; en este caso Reingeniería, como causante del servicio, calidad, confiabilidad y, además, no descuidar las variables de ésta, como sistema integral que es.
- Seguimiento y evaluación, para que exista la retroalimentación.

	PLANOS		
ORGANIZATIVO DINÁMICO	ESTRUCTURAL	FUNCIONAL	COMPORTAMENTAL
Planeamiento	Organigrama	Diagramas	Relaciones Formales Vs Informales
Organización			
Staff (personal)			
Dirección			
Coordinación			
Reportar			
Presupuestación			

Fig. 3.12. Plano organizacional para el cambio y la reingeniería en el sistema de control de seguridad

Consideraciones para con el Personal

Es de gran importancia la elaboración del plan considerando el personal, pues se debe llevar a una conciencia para obtener una auto evaluación de su comportamiento con respecto al sistema, que lleve a la persona a:

- Asumir riesgos
- Cumplir promesas
- Innovar

Para apoyar estos objetivos se debe cumplir los siguientes pasos:

TESIS CON
FALLA DE ORIGEN

Motivar
Se debe desarrollar métodos de participación reflexionando sobre lo que significa la seguridad y el riesgo, así como su impacto a nivel empresarial, de cargo y individual.

Capacitación General
En un principio a los ejecutivos con el fin de que conozcan y entiendan la relación entre seguridad, riesgo y la información, y su impacto en la empresa. El objetivo de este punto es que se podrán detectar las debilidades y potencialidades de la organización frente al riesgo.
Este proceso incluye como práctica necesaria la implantación la ejecución de planes de contingencia y la simulación de posibles delitos.

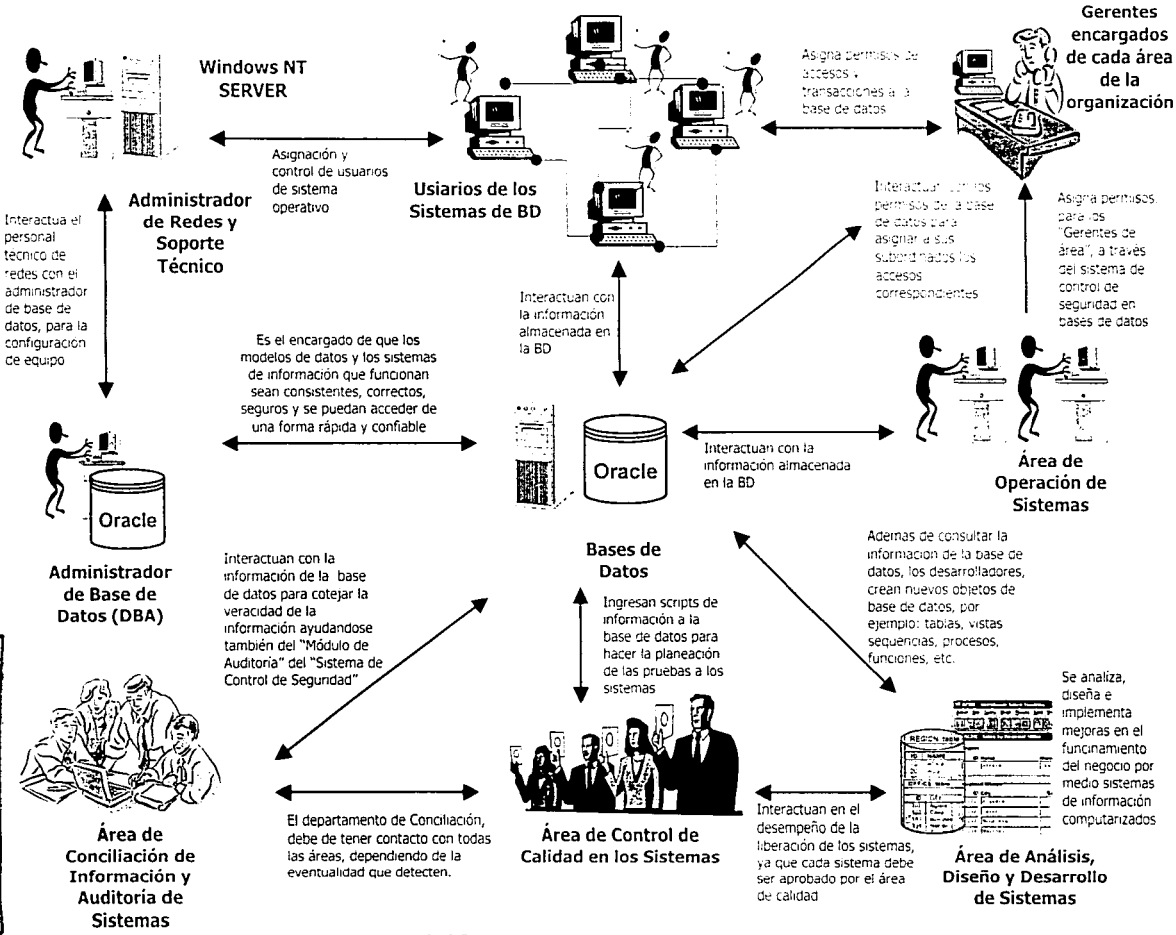
Capacitación de Técnicos
Se debe formar técnicos encargados de mantener la seguridad como parte de su trabajo y que esté capacitado para capacitar a otras personas en lo que es la ejecución de medidas preventivas y correctivas.

Ética y Cultura
Se debe establecer un método de educación estimulando el cultivo de elevados principios morales, que tengan repercusión a nivel personal e institucional.
De ser posible realizar conferencias periódicas sobre: doctrina, familia, educación sexual, relaciones humanas, etc.

Etapas para Implantar un Sistema de Seguridad en Marcha
Para hacer que el plan entre en vigor y los elementos empiecen a funcionar y se observen y acepten las nuevas instituciones, leyes y costumbres del nuevo sistema de seguridad se deben seguir los siguiente 8 pasos:

1. Introducir el tema de seguridad en la visión de la empresa.
2. Definir los procesos de flujo de información y sus riesgos en cuanto a todos los recursos participantes.
3. Capacitar a los gerentes y directivos, contemplando el enfoque global.
4. Designar y capacitar supervisores de área.
5. Definir y trabajar sobre todo las áreas donde se pueden lograr mejoras relativamente rápidas.
6. Mejorar las comunicaciones internas.
7. Identificar claramente las áreas de mayor riesgo corporativo y trabajar con ellas planteando soluciones de alto nivel.
8. Capacitar a todos los trabajadores en los elementos básicos de seguridad y riesgo para el manejo del software enfocado a las bases de datos.

TESIS CON
FALLA DE ORIGEN



3.13 Esquema global del control de la seguridad

148
TESIS CON
FALLA DE ORIGEN

3.2 Pruebas de seguridad y asignación de privilegios

Etapas de Pruebas en el Análisis, Diseño y Desarrollo del Sistema

Al no tener un control de calidad adecuado, el sistema puede tener una gran cantidad de fallas, esto causaría incomodidad al usuario, poca credibilidad en los sistemas de la organización, y lo más importante, no se cumpliría el objetivo, que es aumentar la seguridad en los sistemas de la organización.

Para evitar esto es necesario implementar pruebas al sistema, en todas la etapas de desarrollo del software. El plan de pruebas que involucra al desarrollo del sistema de "Control de seguridad en base de datos" se muestra en la siguiente figura:

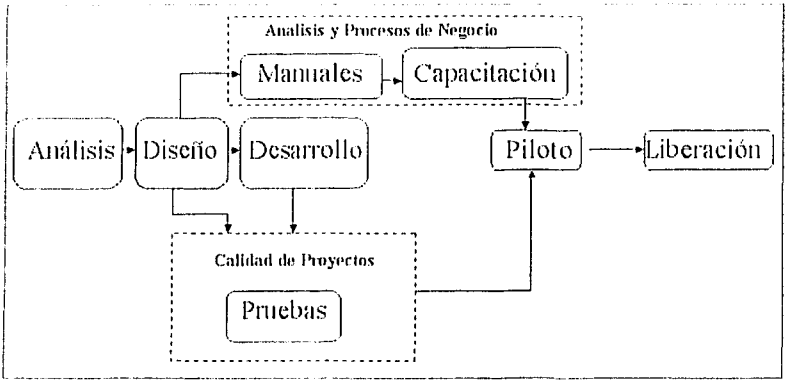


Fig. 3.14 Participación de las pruebas el desarrollo de software.

Los objetivos generales al llevar acabo el plan de pruebas al sistema, son:

- Establecer procesos para la realización y control de pruebas.
- Realizar las pruebas que garanticen la seguridad de la información en la base de datos.

Los beneficios que traerá, implantar el plan de pruebas, es:

- Reducción de tiempo en el proceso de desarrollo del "Sistema de Control de seguridad en bases de datos", ya que se inicia el planteamiento de las pruebas, posterior al diseño.
- Permite una mejora continua en las etapas de diseño y desarrollo.
- Detección y prevención de errores u omisiones previos a la liberación o puesta en producción del "Sistema de Control de seguridad en bases de datos".
- Fortalecer la implementación del sistema con mayor calidad.

La siguiente gráfica muestra el proceso a seguir para efectuar las pruebas al sistema de "control de seguridad" , después de elaborar el diseño técnico.

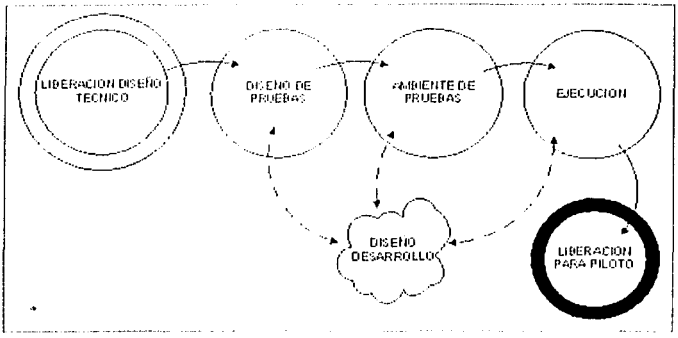


Fig. 3.15 Proceso de diseño de pruebas y ambiente de pruebas

Esta técnica, ayuda a detectar inconsistencias en la recuperación de datos en la base de datos, antes de que los programadores comiencen a desarrollar el sistema, además detecta las posibles fallas del sistema. En la siguiente etapa de pruebas, se crea un ambiente propicio para que los desarrolladores puedan programar de forma correcta, y puedan hacer pruebas individuales en cada uno de los módulos del sistema.

Pruebas entorno al Sistema de Control de Seguridad en Base de Datos

En términos de seguridad informática, una vulnerabilidad se define como cualquier deficiencia de un sistema operativo o aplicación, la cual puede ser explotada por usuarios no autorizados con fines no genuinos (usualmente para ocasionar daño).

Para propósitos de este estudio, se clasificaron a las vulnerabilidades como de alto, medio y bajo riesgo, de acuerdo al grado de severidad que puede tener un ataque que utilice la vulnerabilidad en cuestión. Entre las vulnerabilidades de bajo riesgo se incluyeron a aquellas que permiten la obtención de información secundaria, tal como sistema operativo, versiones de aplicaciones utilizadas, etc.

Entre las vulnerabilidades de medio riesgo se incluyen a aquellas que permiten extraer información más relevante acerca del objetivo, como pueden ser nombres de cuentas de usuario, así como las que permiten ataques que pueden comprometer parcialmente el desempeño y/o buen funcionamiento de los sistemas que usa la organización.

Finalmente, entre las vulnerabilidades de alto riesgo se contemplan las que pueden representar un compromiso total del sistema, permitiendo al atacante el control total del objetivo o, al menos, impedir completamente su funcionamiento.

Es importante tener en cuenta y no pasar por alto los "síntomas" que puedan darse entorno al ambiente de seguridad. Estos "síntomas" ayudan a elaborar un diagnóstico que asegura tanto el aprendizaje como la adaptación.

Un síntoma es uno, de una serie de valores de una variable, que ocurre generalmente cuando algo es excepcionalmente incorrecto. Las variables que se utilizan como síntomas son propiedades del comportamiento o funcionamiento de los organismos u organizaciones. Estas variables se pueden utilizar como también dinámicamente como presíntoma o presagios. Un presíntoma es un comportamiento normal y no aleatorio. [18]

3.3 Beneficios del sistema de control de seguridad

El crecimiento de las organizaciones a través de la historia evidenció la necesidad de desarrollar modelos administrativos prácticos y eficientes, que a la vez que permitieran el incremento del valor de las inversiones de los accionistas, también generaran beneficios económicos, seguridad y respeto a los trabajadores.

Es decir, los beneficios deben de verse reflejados en el desarrollo organizacional y por lo tanto, se refleja también tanto para los inversionistas como para las personas que laboran en la empresa.

Se entiende como desarrollo organizacional "una serie de conceptos de índole diversa, relacionados entre sí y que tiene como objetivo común buscar el desarrollo y la consecución coincidente de los objetivos generales de una organización, con las metas particulares de los individuos que la integran"(Peter Watkins).

Los beneficios de un sistema de seguridad bien elaborados son inmediatos, ya que en la organización se trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- Aumento de la productividad.
- Aumento de la motivación del personal.
- Compromiso con la misión de la compañía.
- Mejora de las relaciones laborales.
- Ayuda a formar equipos competentes.

Aumento de la productividad

Crear condiciones de trabajo adecuadas a las personas encargadas de operar los sistemas de información contribuirá sin dudas a aumentar la eficiencia del trabajo promoviendo la satisfacción y bienestar de la organización. Con este objetivo se ha venido trabajando en el desarrollo de todo el sistema de control de seguridad en base de datos. En realidad este sistema de control de seguridad constituye un paquete de programas que incluye la automatización de todos los factores que involucran la alteración de los datos de todos los sistemas de la organización.

[18] ACKOFF, Russel L., "El arte de resolver problemas", Ed. Limusa, México, 1981 Capítulo 12 (Como mantener los problemas resueltos)

En todos los puestos de trabajo existen responsabilidades y errores humanos que deberían minimizarse conforme a la experiencia y buen funcionamiento de los sistemas. En el diseño del sistema se tuvo en cuenta que las relaciones entre los usuarios y los servidores que almacenan las bases de datos deben ser analizadas en esencia respondiendo a tres preguntas:

¿Tiene conocimiento el usuario de operar adecuadamente los sistemas?

Los diferentes controles que el usuario puede necesitar operar deben ser seguros y fácilmente asequibles.

¿Puede el usuario tener acceso a determinada información?

Los diferentes sistemas que los usuarios necesitan operar deben ser adecuados dependiendo del rango e importancia del usuario, es decir tener una cultura de jerarquías de operadores de sistemas

El diseño de puestos de trabajo debe tener en cuenta la posición y la libertad de acciones en los sistemas. Estas consideraciones provocan requerimientos específicos en lo que se refiere a niveles de trabajo.

Beneficios del sistema de control de seguridad tomando como base los principios de Edward Deming

Los demás puntos que beneficial la implantación del sistema de control de seguridad en base de datos, pueden resumirse en los punto propuestos por **Edward Deming.**

Según Edward Deming (Pionero y profeta de la Calidad Total. TQM - Total Quality Management) el trabajo debe realizarse en un ambiente cómodo y seguro, y que el jefe debe ser justo y comprensivo. Esto es muy importante para Deming, quien también afirma que cuanto mejor se sienta el trabajador mayor será su rendimiento. Desde el comienzo del diseño del sistema de control de seguridad se trata de hacer un ambiente completamente amigable al usuario, para así facilitarle las tareas y disminuir su cantidad de estrés laboral.

Los 14 principios de gerencia de W. Edwards Deming son[19]:

1. Crear un propósito constante hacia la mejora de los productos y servicios (Kaizen = Mejoramiento contínuo), asignando recursos para cubrir necesidades a largo plazo en vez de buscar rentabilidad a corto plazo.

Con este punto se involucra la mejora continua de los procesos que realizan los usuarios de los sistemas, dando por resultado un mejor servicio hacia la empresa y esta hacia sus clientes. El sistema esta pensado a largo plazo, y se logra esto controlando todas las transacciones de información que maneja la organización

[19] Dobyns, Lloyd. 1990. "Ed Deming wants big changes and he wants them fast." Smithsonian 21: 74-80

Creemos que este punto va a afectar específicamente a los departamentos departamento de manejo de información dentro del sistema de producción y a los departamentos de ventas y de servicios de posventa dentro del sistema de servicios al cliente. También puede afectar a otros departamentos como el de cobranzas por ejemplo. Este punto nos indica la necesidad de un constante perfeccionamiento del producto y de los servicios a los clientes.

2. Adoptar la nueva filosofía de la estabilidad económica rechazando permitir niveles normalmente aceptados de demoras, errores, materiales defectuosos y defectos de fabricación.

Este principio afectara a todos los sistemas de una empresa, a todos sus departamentos. Es importante que toda la empresa se preocupe por el cumplimiento de este punto

3. Eliminar la dependencia de inspecciones masivas solicitando pruebas estadísticas inherentes a la calidad en las funciones de fabricación y compras.

Este punto debe aplicarse principalmente al departamento de transacciones de información, dado que es una forma de que el usuario pueda encontrar las fallas en el momento que se producen y arreglar el problema solo. Esto ayudara a acelerar el proceso de elaboración del producto.

4. "Reducir el número de proveedores para el mismo ítem eliminando a los que no califiquen al no aportar pruebas de calidad; o sea terminar con la costumbre de adjudicar negocios sólo sobre la base del precio.

(En términos coloquiales: "Lo barato, sale caro")"
Este principio es aplicable al departamento de compra de nueva tecnología de la empresa. Representa una forma de mejorar la calidad del producto final y ahorrar tiempo en arreglos por defectos en el producto final. En el caso de la organización donde se implanta el sistema de control de seguridad en base de datos esa filosofía se lleva acabo ya que cuentan con lo último en tecnología de almacenamiento de información y base de datos (manejador de base de datos ORACLE).

5. Búsqueda constante de problemas, existentes en el sistema a fin de mejorar los procesos permanentemente.

Observando este principio podemos darnos cuenta de que es muy importante, debe aplicarse a todos los departamentos de cada gerencia puesto que permitirá cumplir con la realización de todas las tareas sin tener que volver atrás en caso de hallar un problema, este será resuelto si bien surge.

6. Instituir la capacitación continua en el trabajo. Desarrollar e implementar planes de adiestramiento y mejora continua al personal.

Este punto también debe aplicarse a las partes gerenciales de la empresa, es importante para la seguridad de los empleados. El sentirse mas capacitados los ayudara a realizar mejor sus tareas, sintiéndose mejor consigo mismos. Además es importante que estén actualizados en cuanto al

mejoramiento de los métodos para realizar sus tareas que van surgiendo con el paso del tiempo.

7. Concentrar la supervisión en ayudar al personal a desempeñar mejor su trabajo. Tomar medidas inmediatas en cuanto a imperfecciones, necesidades de mantenimiento, malas herramientas, u otras condiciones inadecuadas para la calidad.

Este principio se aplica específicamente a los gerentes de área y al gerente general de la organización. En muchas ocasiones, los gerentes suelen designar este trabajo a alguno de los empleados, el cual lo elegirá con la ayuda de el sector de recursos humanos y quien deberá tener ciertas características como ser reconocido por sus compañeros.

8. Estimular la comunicación eficaz, de dos vías, y otros medios que eliminen temores en toda la organización y ayudar a las personas a trabajar juntas para servir los propósitos del sistema.

Este punto debe ser llevado a cabo por el gerente con la ayuda de los gerentes de área y con el asesoramiento infaltable del sistema de recursos humanos, el cual funcionara como nexo y trabajara con los empleados para poner en marcha esta idea sin interferencias. El sistema de control de seguridad estimula este punto ya que al usuario se le pueden ir asignando tareas conforme aumente su conocimiento en la funcionalidad del negocio.

9. Romper las barreras existentes entre los departamentos de la empresa estimulando trabajos en equipo, congregando esfuerzos de áreas diferentes: investigación, diseño, ventas y producción.

Esta tarea esta totalmente apuntada a la gerencia, quien se ocupara, al igual que en el punto anterior con recursos humanos, de fomentar esta forma de trabajo y mejorando la comunicación.

10. Eliminar el uso de objetivos numéricos, afiches y lemas en los cuales se pide nuevos niveles de productividad sin dar los métodos y proveer las herramientas y entrenamiento necesarios.

La tarea de terminar con los métodos de motivación que se utilizaban, siempre será trabajo para la gerencia.

11. Mejorar permanentemente la calidad y la productividad.

Indudablemente con la implementación del sistema de control de seguridad es lo que se alcanzará

12. Eliminar las barreras que le impiden al trabajador el derecho de sentirse orgulloso de su destreza.

La destreza del usuario de sistemas será aumentada a un punto en el que se interesará en el funcionamiento de la organización.

13. Instituir un vigoroso programa de educación y auto mejora.

TESIS CON
FALLA DE ORIGEN

En este punto también deberá ser la gerencia, con la ayuda del sector de recursos humanos, quien se ocupe de la puesta en practica del mismo.

14. Definir el compromiso permanente de la alta gerencia con la calidad y productividad y su obligación de implementar todos estos principios.

Aquí es el gerente general el que debe concretar este objetivo. Este punto es uno de los más difíciles al implantar el sistema de control de seguridad, ya que el gerente es quien decide las mejoras de la organización.

3.4 Escalabilidad y prospectiva del sistema

Al resolver algún problema, es muy difícil que permanezca en ese estado, por el contrario, las condiciones cambiantes del medio tienden. Por lo tanto al implantar el sistema de control de seguridad, no solo se revisaron y se estudiaron las soluciones previas en la organización en donda se implanto, sino que hay que mantenerse alerta y explorar constantemente el horizonte para identificar los nuevos problemas que se presentan o que se presentarán.

Las causas por las cuales, no se llega a un completo control de seguridad en la información almacenada en las bases de datos son:

- La información que se uso para tomar la decisión estaba equivocada y por consiguiente, el subsistema de información requiere cambio a fin de que no se repita ese tipo de error.
- El proceso de toma de decisiones puede haber sido defectuoso.
- Puede ser que la decisión haya sido atinada, pero no se la puso en práctica como se proponía.
- El ambiente cambio de manera imprevista.

Estas causas se toman con base en las causas por las cuales no se llega a un objetivo planteado de Acoff Russel[10].

En el enfoque global para el sistema de control de seguridad, el punto de convergencia de la escalabilidad, se basa en los sistemas informáticos. La habilidad para responder rápidamente a condiciones de negocio cambiantes requiere sistemas y plataformas que ofrezcan los más altos niveles de flexibilidad.

Esto significa una infraestructura que soporte la implementación rápida de nuevos productos y servicios, y ofrezca la posibilidad de incrementar o disminución de la capacidad computacional casi instantáneamente. Las organizaciones que implementan sistemas altamente escalables cosechan los frutos de los beneficios de una agilidad mayor y una habilidad mejorada dramáticamente para implementar recursos que ellos necesitan cuando las nuevas oportunidades surgen y las condiciones cambian.

[10] ACKOFF, Russel L., "El arte de resolver problemas", Ed. Limusa, México, 1981 Capitulo 12 (Como mantener los problemas resueltos)

TESIS CON
FALLA DE ORIGEN

Debido a que las condiciones del negocio cambian rápidamente, la habilidad para adecuar fácilmente el crecimiento es también esencial. Tradicionalmente, han habido 2 enfoques para expandir los sistemas de información: escalar lateralmente o escalar hacia arriba (scaling up). Cada enfoque ofrece diferentes ventajas. El sistema informático en que se apoya el control de seguridad, tiene un escalamiento vertical

El escalamiento lateral es un medio de aumento de capacidad al agregar hardware para que la operatibilidad del sistema sea difundido a más personas. El escalamiento lateral es ideal para implementaciones rápidas de sistemas activos más pequeños y provee a las organizaciones de todos los tamaños, la agilidad necesaria para responder rápidamente a requerimientos cambiantes de negocios.

El escalamiento vertical (scaling up) es un enfoque poderoso para incrementar el rendimiento y capacidad por medio de técnicas de optimización en la recuperación y manipulación de datos. Este escalamiento es ideal para aplicaciones críticas que requieren de los más altos niveles de confiabilidad y rendimiento, para aplicaciones grandes de bases de datos u otras cargas de trabajo no particionables y para reducir la complejidad de infraestructura TI. Los beneficios del escalamiento vertical en el sistema informático de control de seguridad es el ágil acceso a la información por medio de técnicas de optimización en la recuperación de datos, migrar a una plataforma web, para que los usuarios puedan acceder al sistema desde cualquier terminal que cuente con internet, o mejorar el ambiente en general para un mejor entendimiento en el funcionamiento del sistema.

En algunos casos la más importante característica de un sistema altamente escalable es su índice de precio/rendimiento. Al final, la manera en como se refleja que la organización medirá el valor de su infraestructura de información es observando la relación entre la cantidad de dinero que ha invertido y los niveles de rendimiento que ha alcanzado.

Los negocios hoy en día, demandan una clase diferente de soluciones de bases de datos. Rendimiento, escalabilidad y confiabilidad son esenciales y el tiempo para comercializar es crítico. Cuatro características son esenciales para lograr obtener altos niveles de escalabilidad que las empresas de hoy en día necesitan. Estas son:

- La capacidad de manejar grandes volúmenes de información, y carga de trabajo.
- La capacidad de ofrecer altos niveles de rendimiento.
- La capacidad de crecer fácil y rápidamente.
- Un índice de precio/rendimiento que corresponda con las normas de la industria.

Las funciones a realizar por un sistema inteligente que administre los accesos a la información, día a día debe de adaptarse a las necesidades que las organizaciones demandan, y proveer un valor agregado a el uso de las aplicaciones computacionales desarrolladas para un fin en específico. En general, a medida que se madura el uso de los sistemas usados para el control de seguridad, y se concientiza al personal, en la importancia del uso de políticas y estándares, puede dar como resultado, directa o indirectamente que el proceso de experiencia en incidentes registrados por el sistema provea soluciones firmes.

TESIS CON
FALLA DE ORIGEN

El aseguramiento en el cumplimiento de los siguientes puntos, dará como resultado que el sistema global para el control de la seguridad logre permanecer como una solución a los incidentes registrados en las bases de datos:

- Parametrizar la alimentación de la Base de Datos por parte de los Operadores y Usuarios para garantizar su confiabilidad.
- Alimentar directamente la Base de Datos con aquellos datos o información que escape del dominio del Usuario u Operador para asegurar su representatividad y utilidad para fines de análisis y Mercadeo.
- Coordinar el diseño de Programas o Aplicaciones con el Área de Informática para preservar la compatibilidad de los sistemas y facilitar el uso de la Base de Datos.
- Depurar continuamente la Base de Datos para garantizar su confiabilidad.
- Respaldar todo registro para asegurar la preservación de los datos.
- Concienciar al usuario sobre los usos y la utilidad de la Base de Datos para propiciar su máximo aprovechamiento, por él más amplio universo de Gerentes, Unidades y Ejecutivos
- Analizar la información que emana periódicamente de la Base de Datos, cruzándola con aquella que generen los estudios de Mercados, para conformar alertas e informes oportunos.
- Elaborar los Informes o Reportes con el propósito de informar a las Gerencias oportunamente y documentar el Plan Operativo.
- La ejecución de éstas funciones, además de que le da beneficios a la organización por tener accesible y segura su información, es evaluar la posibilidad de hacer escalable el sistema a otros niveles.

TESIS CON
FALLA DE ORIGEN

Planeación de Escenarios

La proyección de escenarios para la organización que tenga planeado incrementar su nivel de seguridad informática, debe de considerar los siguientes elementos:

Variables primarias:

- Crecimiento de los sistemas en la organización: Técnicas sobre los procesos de seguridad y políticas de uso en los sistemas.
- Recursos para obtener tecnología de punta: Manejo e implantación de tecnología de punta, tanto en software como en hardware.

En este punto, es necesario determinar un ambiente de hardware y software óptimo para responder a las necesidades de cada organización en materia informática, y que sea útil en un lapso de tiempo considerable. Los puntos más relevantes son:

- Hardware
  - Tamaño y capacidad
  - Medición y evaluación de computadoras
  - Compatibilidad del equipo
  - Factores financieros
  - Mantenimiento y soporte

- Software (aplicación y/o ambiente de desarrollo)
  - Cumple con los requerimientos del usuario
  - Flexibilidad a cambios de requerimientos del usuario
  - Soporte del proveedor

Variables Secundarias:

- Capacitación a los usuarios de los sistemas.
- Optimización en el proceso de asignación de sistemas.
- Disminución en las dependencias laborales con personal especializado en bases de datos.
- Mayor seguridad en los sistemas, por el control de accesos, detección oportuna de fraudes y técnicas de encriptación.

TESIS CON
FALLA DE ORIGEN

Planeación de escenarios año 2020

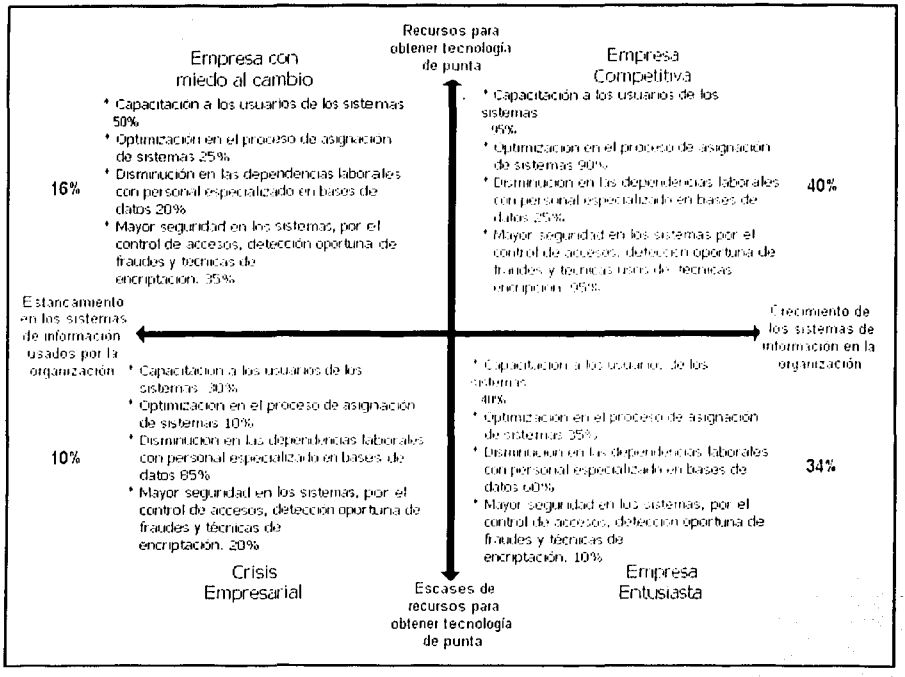


Fig. 3.16 Planeación de escenarios para el sistema global en el control de seguridad en base de datos.

El esquema para la planeación de escenarios propuesto, considera los siguientes rubros:

- Empresa competitiva.
- Empresa con miedo al cambio.
- Crisis empresarial.
- Empresa entusiasta.

Dentro de cada uno de éstos rubros se describen los porcentajes para cada una de las variables secundarias.

TESIS CON
FALLA DE ORIGEN

Reglas para que se cumplan los escenarios

1er Escenario, Empresa Competitiva.- En el primer escenario, donde la organización tiene recursos para obtener tecnología de punta y además se tiene un crecimiento en los sistemas de la organización, dará como resultado una constante capacitación de los empleados para poder soportar el avance tecnológico en los sistemas, además con el sistema informático de control de seguridad, el proceso de asignación de las aplicaciones computacionales para el procesamiento de información será más ágil y de forma sencilla, por ende tendrán mayor seguridad en el manejo de información. En conclusión, en éste escenario se observa que la empresa ofrece mejores expectativas de crecimiento y estabilidad económica así como mayores oportunidades de empleo, y crecimiento.

2do Escenario, Empresa entusiasta.- Este escenario muestra que aunque la empresa tiene una demanda en el procesamiento de la información, no cuenta con los recursos suficientes para cumplir con sus necesidades tecnológicas, esto conlleva a que no exista a un buen nivel en la capacitación a los usuarios de los sistemas y las dependencias con el personal especializado es mayor, tampoco se podría contar con un buen nivel de seguridad, en general la empresa subsiste gracias al entusiasmo, pero no se puede clasificar como una empresa competitiva.

3er Escenario llamado "Crisis empresarial", ocurre cuando no hay desarrollo en la empresa, por consecuencia el procesamiento en su información es mínima, además de esto, no tienen los recursos suficientes para invertir en tecnología, si no por el contrario, su objetivo principal, es seguir manteniendo la empresa viva en el mercado. Este clima laboral no da un crecimiento profesional a sus empleados, por el contrario, obliga a que estén en una búsqueda constante de crecimiento en otras organizaciones. En lo que respecta a los sistemas de información, generalmente son obsoletos, y no tienen los requerimientos necesarios para que se pueda trabajar de forma segura y confiable, lo que ocasiona información inconsistente, que no sirve de mucho para sacar a la organización de la crisis en la que se encuentra.

4to Escenario llamado "Empresa con miedo al cambio", se observa que a pesar de tener recursos económicos para invertir en tecnología para el desarrollo de la empresa, deciden no hacerlo generalmente por miedo al cambio o por no querer cambiar su forma de trabajo en la organización, ya que de hacerlo, ponen en riesgo el empleo de los trabajadores de la organización.

TESIS CON
FALLA DE ORIGEN

Tabla del escenario llamado "**Empresa Competitiva**"

Descripción	2005	2010	2020
Capacitación a los usuarios de los sistemas	A partir de la capacitación en las políticas de seguridad informática y operación del control de acceso, los usuarios han tomado el cambio de la mejor forma ya que comprueban la efectividad de la interfaz y la rapidez para asignar accesos a la información.	Se capacita a los usuarios para hacer simulacros de pérdidas de información, y se hacen fraudes ficticios para ser rastreados por medio de la auditoria generada por el sistema. Una vez mas se comprueba que el diseño y las políticas entorno a proteger la información, son aceptadas y valoradas por los directivos de la organización.	Se capacita a los usuarios, no solo para que sepan manejar el sistema y rastrear fraudes por medio de la auditoria, sino también se les capacita para instalarlo. La capacitación es dada a todas las sucursales de la organización y se implantan nuevas políticas de acceso remoto a los sistemas, ya que el sistema se implanta en Internet.
Optimización en el proceso de asignación de sistemas	Una vez hecha la asignación de los accesos, y la carga de información, se asignan personas con permisos de suministrar acceso a los sistemas, además se crea el grupo de solución a incidentes sobre la información almacenada en la base de datos.	El ambiente global para el control de la seguridad a los sistemas, es dado por el sistema informático de control de accesos en un 80%, y se afinan las políticas de seguridad para agilizar aun mas el suministro de acceso a la información, sin perder el objetivo inicial.	No se permitirá otorgar privilegios a ningún usuario, si no es por medio del sistema de control de seguridad en base de datos. El proceso de asignación de sistemas es explotado al máximo, con esto disminuye la inconsistencia de información por mal manejo de la misma, por tener permisos no concedidos.
Disminución en las dependencias laborales con personal especializado en bases de datos.	La asignación de privilegios al sistema son monitoreados constantemente por el "Administrador de la Base de Datos", en un 90%.	La asignación de permisos es otorgada solamente por un personal no especializado en base de datos en conjunto con el "Administrador de la base de datos".	La asignación de permisos a los sistemas es otorgada únicamente por el personal o el área operativa de la empresa. La asignación de permisos es otorgada y manipulada por el gerente de cada departamento. Con esto el área operativa de sistemas de la organización solo se dedicará a auditar las transacciones.
Mayor seguridad en los sistemas, por el control de accesos, detección oportuna de fraudes.	La seguridad es aumentada de un 30% a un 80%, por implantar políticas de seguridad y técnicas de encriptación por el sistema de control de accesos	La detección oportuna de fraudes reduce las pérdidas económicas en la organización en un 50%	La implantación de las políticas de seguridad dan como resultado una óptima solución a problemas de pérdida de información en un 70%. La seguridad en la información es controlada en su totalidad, y son registrados cada uno de los intentos de fraudes intencional o accidentales.

FALLA DE ORIGEN
NO SISTEMA

Tabla del escenario llamado "**Crisis Empresarial**"

Descripción	2005	2010	2020
Capacitación a los usuarios de los sistemas	A pesar de que se les imparte la capacitación, los usuarios no dan lugar a cambiar su estilo de trabajo.	El sistema es usado, solo por el área de operación de sistemas, dejando el sistema anterior para el resto de los usuarios	Se decide que el sistema será un apoyo para tener control de los accesos, y solo será usado por el administrador de la base de datos y por el área de operación de sistemas, en la parte de auditoria de transacciones
Optimización en el proceso de asignación de sistemas	Por la apatía entre los usuarios de sistemas, y por dar prioridad a otros proyectos, la carga inicial para la asignación de sistemas, es demorado y solamente usado para los sistemas nuevos.	El usuario piensa que el nuevo sistema es complejo y lento en la tarea de asignación de accesos a los demás sistemas de información, por lo que decide dejar esa labor al administrador de base de datos.	A pesar de que el sistema esta puesto en producción, no es usado más que en un 50%. La persona que más usa este sistema, es el administrador de base de datos, y lo usa como un apoyo para el control interno de su administración.
Disminución en las dependencias laborales con personal especializado en bases de datos.	Los usuarios de operación de sistemas, no dejan de pedir ayuda al administrador de la base de datos para realizar su tarea de asignación de permisos sobre los nuevos sistemas.	A pesar de que los usuarios de operaciones, encargados de la auditoria en los sistemas, monitorean constantemente la base de datos, por el mal uso del sistema, no se detectan fraudes a tiempo. Por lo que es necesaria la intervención nuevamente del administrador de la base de datos	La asignación de permisos, y monitoreo y control de auditoría es explotada a un 60% de la capacidad total del sistema, lo que más a resultado de todo el proyecto, es tener un control interno de accesos a los sistemas y transacciones realizadas.
Mayor seguridad en los sistemas, por el control de accesos, detección oportuna de fraudes y técnicas de encriptación.	La única ventaja para dar mayor seguridad, son las técnicas de encriptación de datos, y el temor de los usuarios, por ser detectados haciendo fraude de información, por la puesta en producción del sistema	La detección oportuna de fraudes reduce las pérdidas económicas en la organización en un 20%, esto originado básicamente por el cambio de políticas y sanciones por causar inconsistencia de la información.	Es aumentada la seguridad en un 50%, y a pesar de que la detección de fraudes no es oportuna, se sabe quien causo las alteraciones de la información a la base de datos, sea intencional o no intencionalmente.

TESIS CON
FALLA DE ORIGEN

Tabla del escenario llamado "**Empresa Entusiasta**"

Descripción	2005	2010	2020
Capacitación a los usuarios de los sistemas	La capacitación de los usuarios es paulatina, y su cultura va cambiando ya que se les hace ver los beneficios del sistema.	La capacitación es incrementada conforme va creciendo el número de los sistemas en la organización y además a los nuevos empleados se les impone el uso de éste sistema.	La capacitación es impuesta para todos los empleados, no importando rangos, ni conocimientos en la operación de los sistemas. Logrando que todos tengan conocimiento del funcionamiento del sistema de control de seguridad, tanto en la administración de permisos, como el la auditoria generada por el sistema.
Optimización en el proceso de asignación de sistemas	El sistema es puesto en producción y se tiene un control de todos los objetos de base de datos que tienen permisos los usuarios, logrando con esto eficiencia en la tarea de asignar nuevos sistemas y se reducen los errores humanos.	Los errores humanos, reducidos a un 10%, además, los sistemas son liberados más rápidamente hasta un 70% más rápido que con el sistema anterior	El tiempo de asignación es reducido hasta un 90%, además el proceso de auditoria, detecta accesos que hacen lenta la base de datos, dando pie a que se cambie la estructura del perfil del usuario para optimizar los procesos.
Disminución en las dependencias laborales con personal especializado en bases de datos.	Los usuarios de operación de sistemas, se interesan por el nuevo sistema de control de seguridad, y cada vez más, tienen la agilidad para usarlo asignar accesos, y monitorear la auditoria. Quitando carga de trabajo al administrador de la base de datos hasta un 50%	Se planea para que los usuarios en general, ya no tengan dependencias con los usuarios de operación de sistemas, sino con sus gerentes de área, ya que éstos serán los que les otorguen los accesos. La auditoria sigue encargada de operación de sistemas.	La dependencia de los usuarios, ya no es en ningún aspecto con el administrador de la base de datos, sino con su gerente de área, y los gerentes de área con el área de operación de sistemas.
Mayor seguridad en los sistemas, por el control de accesos, detección oportuna de fraudes y técnicas de encriptación.	El aumento en el control de la seguridad es visto desde una perspectiva a bajo nivel, ya que las técnicas de encriptación permiten que los usuarios de operación de sistemas, no conozcan los passwords de los demás usuarios, Además la auditoria	La detección oportuna de fraudes reduce las pérdidas económicas en la organización en un 70%, esto originado básicamente por el cambio de políticas y sanciones por causar inconsistencia de la información.	Es aumentada la seguridad en un 80%, y la detección de fraudes es oportuna, con esto se sabe quien causo las alteraciones de la información a la base de datos, sea intencional o no intencionalmente, para tomar medidas sobre éste tipo de transacciones.

FALLA DE ORIGEN
TESIS CON

Tabla del escenario llamado "**Empresa con miedo al cambio**"

Descripción	2005	2010	2020
Capacitación a los usuarios de los sistemas	Se da la capacitación a los usuarios de sistemas únicamente de los procedimientos básicos para operar el sistema de control de accesos, y se implementan las políticas únicamente para apoyar a éste sistema.	Los usuarios mantienen en una postura estática respecto al uso dinámico del control de accesos y usan el sistema únicamente para auditar el uso de las aplicaciones.	Definitivamente los usuarios desechan la posibilidad de usar el sistema de control de accesos y políticas de seguridad, por lo que la organización capacita únicamente al personal técnico especializado en base de datos.
Optimización en el proceso de asignación de sistemas	La optimización únicamente se da en un 25% ya que el uso de políticas y sistemas entorno a la seguridad, es usado por el departamento de desarrollo de sistemas de la organización.	El uso del sistema ha permanecido únicamente por imposición de los directivos de la organización, pero realmente el proceso de asignación de aplicaciones, sigue siendo por parte del administrador de base de datos.	Se erradica el sistema de control de accesos ya que los usuarios piensan que es más tedioso y tardado el acceso a la información por las políticas que deben de cumplirse.
Disminución en las dependencias laborales con personal especializado en bases de datos.	El personal especializado en base de datos, se ve en la tarea de apoyar a los usuarios por la premura que de debe de tener en el acceso a la información, el sistema de control de acceso se monitorea en tareas que no tengan prioridades.	El personal especializado en base de datos sigue asignando aplicaciones a los sistemas, por, lo que los usuarios no dudan en pedir ayuda. Los usuarios no respetan la políticas de seguridad por la confianza entre el personal técnico de la organización.	La organización se ve en la necesidad de invertir en la contratación de más gente especializada en el manejador de base de datos usado, ya que no se dan abasto en dar soporte a la base d e datos, esto por el crecimiento de usuarios.
Mayor seguridad en los sistemas, por el control de accesos, detección oportuna de fraudes y técnicas de encriptación.	La detección oportuna de fraudes no se da, los fraudes son detectados hasta después de un lapso de tiempo considerable, esto ocasiona pérdidas que la organización tiene que cubrir. El resultado de esto es el mal uso del sistema de control de accesos, en el módulo de auditoría.	Una de las principales tareas del personal de sistemas es detectar los fraudes, esta tarea la realizan explorando la información directamente en la base de datos, lo que ocasiona una pérdida de tiempo muy grande, y este tiempo es costoso para la organización, además de no detectar los fraudes oportunamente.	La seguridad en los sistemas se ve afectada por el mal procesamiento de la información a causa de no usar el sistema de control de accesos, esto ocasiona que la base de datos contenga datos inconsistentes. El mal procesamiento de ésta información es porque el personal especializado en base de datos no puede controlar los permisos sobre los objetos de los sistemas, ya que los usuarios han crecido.

TESIS CON
FALLA DE ORIGEN

Conclusiones Capítulo III

En el primer apartado se observo que todo proceso de una organización debe contener actividades de control de seguridad. Cualquier proceso de la organización con o sin la aplicación de reingeniería no puede permanecer sin los controles de seguridades tanto en sus datos como en sus componentes. La ausencia de controles se presenta siempre como un proceso rediseñado y casi siempre en procesos sin ningún tipo de aplicación de herramientas de mejoras de la eficiencia y productividad. La reingeniería de software es una herramienta metodológica excelente, viable y con grandes resultados y mejoras dramáticas, esto aplicado al esquema global para el control de la seguridad, dio como resultado que la seguridad aumentara en un 80%. De igual forma, procesos que no hayan pasado por reingeniería pueden presentar ausencias de controles si estos no han sido considerados estratégicamente.

En lo visto en el apartado 3.2, se concluye que las pruebas entorno a la seguridad se deben de implementar como un diseño desde la etapa en la que se modela el. Además, en lo que se refiere a los accesos, es necesario aplicar distintas técnicas de pruebas, por ejemplo pruebas aleatorias de accesos a los sistemas para verificar su autenticidad y actualidad.

Por lo mencionado en el apartado 3.3 los beneficios de tener un sistema de seguridad nunca podrán ser medidos completamente, porque la mayoría de las empresas no sabrán realmente "cuando" alguien tratará de quebrantar sus seguridades. Sin embargo, es fácil determinar objetivamente que los beneficios serán grandes, producto de los costos evitados. Es entonces, en estas circunstancias, donde los sistemas de seguridad son invaluables. Las únicas ventajas y desventajas se podrían encontrar en los sistemas de seguridad están dadas en la alternativa de seguridad que se implemente, la cual brindará mayor o menor seguridad a sus procesos. La otra alternativa que se puede ofrecer, es la de sencillamente no tener ningún sistema de seguridad; lo cual resultaría absolutamente negligente.

Finalmente en la sección 3.4 se llega a la conclusión que si la infraestructura de información no fue desarrollada pensando en escalabilidad, la compañía pondrá tener obstáculos en el camino para seguir compitiendo. La incapacidad de escalar rápida y eficientemente puede significar que las oportunidades se vuelvan no adecuadas y que los recursos costosos de tecnología de la información no se aprovechen.

TESIS CON
FALLA DE ORIGEN

Bibliografía Capítulo III

- Perter Bishop "Conceptos de Informática" Ediciones Anaya Multimedia, S.A. 1989 Capitulo I

- Prof. Carlos A. Fernández y Fernández "Instituto de Electrónica y Computación", Universidad Tecnológica de la Mixteca (Apuntes)

- Díaz Gustavo, "Como operar el cambio vía reingeniería", Revista Acta Académica, Universidad Autónoma de Centro América, número 22, Mayo 1998

- Kendall &Kendall., Análisis y Diseño de Sistemas PrenticeHall Hipanoamericana, S.A. de C.V. 1997

- Hersey, Paul. "Estilo Eficaz De Dirigir : Liderazgo Situacional, No Existen Dos Situaciones Iguales / Paul Hersey Y Ken H. Blanchard. México, D.F. : Idh Ediciones, C1981.

- Dobyns, Lloyd. 1990. "Ed Deming wants big changes and he wants them fast." Smithsonian 21: 74-80

TESIS CON
FALLA DE ORIGEN

Conclusiones Generales

La información dicen que es poder, y como las bases de datos son un almacén de información también almacenan poder, por lo que han sido objeto de intentos de acceso no autorizados desde su nacimiento. Por eso, las bases de datos, se han dotado de unos mecanismos que hacen posible la gestión de la seguridad en el acceso a la información que almacenan. Para tener un elevado control de seguridad, en cualquier organización es necesario inyectar recursos materiales y tecnológicos, así como establecer políticas internas de la organización como es implantar técnicas de prevención de delitos en materia de información. Estas técnicas, no son difíciles, pero en el 90% de las ocasiones, las empresas no ponen en práctica estos métodos porque reducen el rendimiento de la red u otras excusas similares de pobre argumento.

En el presente trabajo de investigación, conforme a lo descrito en el capítulo 1, se ha hecho ver que la información es el punto en el cual converge el funcionamiento de toda organización. Para ello, se ha reconocido, que la forma de consultarla y procesarla de forma más ágil, es por medio de computadoras, además cierta información puede ser confidencial, y en tal caso, hay que protegerla ya que puede ser mal utilizada o divulgada, y en algunas ocasiones puede estar sujeta a robos, sabotaje o fraudes.

Al considerar el manejo de la información, se hizo referencia al lenguaje estándar para base de datos, e introducción a las bases de datos relacionales, para tener una visión de los sistemas de control para la seguridad de base de datos.

De acuerdo a lo investigado en el capítulo dos, se observo que planear la seguridad en los sistemas de información, es una tarea que se debe estudiar cuidadosamente. La forma en como se realizo este estudio, fue por medio de un análisis estructurado de la metodología Yourdon, al final del análisis se llego a la conclusión que las medidas de seguridad deben ser adoptadas de acuerdo a las necesidades de la organización. El desarrollo del sistema de control de accesos a bases de datos, dio como resultado una administración de seguridad eficiente y óptima para la organización en donde se implanto, ya que la asignación de privilegios ahora la otorgan los encargados de área y no por parte del administrador de base de datos.

El tipo de plan tomado para el desarrollo de este sistema es un tipo de plan operativo, porque hace que la operación en cuanto al control de la seguridad sea automatizado, además se desarrollará en un periodo de tiempo de aproximadamente cinco meses, con lo que se considera que es de corto plazo. La categoría del plan operativo a poner en marcha es un plan fijo porque se basa en decisiones programadas y son utilizados para manejar actividades recurrentes.

Además se observa que las empresas que adoptan un plan global para el control de la seguridad enfocados en base de datos, tienen una tipología de planeación preactivista, ya que piensan que la tecnología es la principal causa de cambio, y tratan de hacerlo lo más rápido posible, es decir, están a la vanguardia en avances tecnológicos.

Se hizo notar en el capítulo tres, que para lograr mejores resultados en el uso de medidas de seguridad, es importante el manejo de políticas de seguridad. Cabe señalar que tanto las políticas de seguridad en el acceso, como los sistemas de encriptamiento, dependen en gran

TESIS CON
FALLA DE ORIGEN

medida de la habilidad que se tenga para implementarlos, este hecho es incluso más relevante que el costo de los equipos que se utilicen para desarrollar el sistema de seguridad.

Una prueba notable al respecto es que el auge del comercio electrónico ha obligado a las empresas que dependen sustancialmente de esta clase de negocios, a replantear las políticas de conexiones seguras y de métodos de autenticación, cada vez más complejos y confiables.

Con base a lo visto aquí, se puede deducir que no se debe dar más importancia a la seguridad externa que a la interna; ya que la divulgación de información, ya sea voluntaria o involuntaria, es otro tipo de amenaza.

En conclusión, el objetivo de la seguridad es garantizar la privacidad de la información y la continuidad del servicio, tratando de minimizar la vulnerabilidad de los sistemas, o de la información contenida en ellos; así como tratando de proteger las redes privadas y sus recursos mientras que se mantienen los beneficios de la conexión a una red pública.

Con todo lo aprendido a lo largo de este trabajo, es posible ahora percibir la gran relevancia del tema de la seguridad informática, y que es propia responsabilidad aplicar los conceptos; así como investigar cuáles son los últimos problemas de seguridad reportados.

El modelo administrativo aplicado a la organización que adopta el esquema planteado de control de seguridad, es obligadamente de reingeniería porque aunque, el proceso de "Control de Seguridad de Base de Datos", ya esta implementado de forma técnica y tecnológica en los manejadores de base de datos, no es un proceso automatizado para las necesidades de cada negocio. Con esto se trata de innovar un proceso ya establecido y crear un producto de valor para los usuarios de los sistemas.

En el año en curso por la intervención de los Estados Unidos en el conflicto con Irak, las estrategias militares toman una importancia sin precedente para lograr los objetivos de las tropas norteamericanas. Estos objetivos no pueden ser posibles sin una comunicación eficiente y confiable entre los miembros que toman parte en las tácticas de guerra, por esto la información transmitida y almacenada, debe de cumplir con la confidencialidad e integridad, autenticidad del transmisor de la información, y autorización de codificar la información recibida. Estos puntos forman parte del esquema de seguridad implementado por el sistema informático de control de accesos.

De acuerdo con el objetivo inicial, se afirma que con la implantación del esquema global de control de seguridad en bases de datos dentro de una organización, dio como resultado:

- Aumento de la Productividad.
- Compromiso con la misión de la compañía
- Ayuda en la formación de equipos competentes.

TESIS CON
FALLA DE ORIGEN

Análisis de productividad en el control de accesos a la base de datos

Productividad es la producción generada a partir de unos medios determinados. En la actualidad, se reconoce que el aumento de la productividad es el factor decisivo para aumentar la calidad de vida de la población. La productividad es la principal fuente de crecimiento económico, y a su vez, determina en gran medida el grado de competitividad que tienen las organizaciones.

La clave del éxito de las organizaciones más productivas, esta con base en la administración de los accesos que se tengan a las bases de datos y la capacidad de procesar la información contenidas en las mismas, y no (como muchas organizaciones piensan), en la tecnología de la información. De igual manera, la clave del liderazgo de una organización ha pasado de situarse en la cuantía de su inversión en informática, a su capacidad de gestionar la información. En éste concepto el aumento en la productividad a partir del control global de la seguridad se ve afectada en los siguientes casos:

- El tiempo de respuesta en la solución de incidentes aumenta en un 70%.
- Las fallas de los sistemas generados por pérdidas en la información diminuyen a un 10%.
- Los delitos en los sistemas, fueron detectados en un 95% por él modulo de auditoría.
- El mal uso de claves de acceso fue reducido en un 80%
- La información inconsistente generada por interrupción en los procesos de la base de datos (causadas por fallas en la energía eléctrica, pérdida del enlace con el servidor, etc.), se reduce a un 20%.

Compromiso con la misión de la compañía

La misión de la organización se ve cumplida en que la información generada por los sistemas logra los mejores niveles de confiabilidad a través de la medición y mejora continua de los productos y los procesos gestionados por el sistema de control de seguridad.

Además, la reducción de aproximadamente 50% en términos reales en los costos unitarios por mantenimiento en la información y detección de errores, se han traducido en ganancias reales en la compañía, este punto es el más importante para que se cumpla la misión.

Ayuda en la formación de equipos competentes.

Un equipo competente se logra a través del tiempo y de la

Las mejoras en las relaciones laborales, se traduce en atraer y retener a el melos mejores ingenieros del país con una perspectiva de largo plazo para todos nosotros aún a pesar de la presión migratoria y de costos proveniente de Estados Unidos. A la fecha únicamente hemos perdido a 3 ingenieros por esta causa.

TESIS CON
FALLA DE ORIGEN

Además, se concluyen los siguientes puntos:

1) Al apoyarse en un sistema de control de seguridad, no eliminan las funciones del proceso administrativo, ni las tareas de auditoría interna, por el contrario, los integra dentro de un marco destinado a la creación de sistemas más eficientes.

2) Es necesario que en todo emprendimiento informático enfocado a los sistemas de información, debe estar presente, desde las ideas preliminares del diseño, el concepto de seguridad de la información.

3) Contar con un sistema de información seguro, es de vital importancia para cualquier empresa, ya que mediante éste se podrá satisfacer las necesidades de información, según lo requieran los usuarios.

4) Tener un nivel de seguridad aceptable en una organización, a través de un plan global de control de seguridad, ayudará a evitar y prevenir pérdidas a la empresa.

6) Para el cumplimiento adecuado del plan de control de seguridad, es necesario la combinación efectiva del personal, equipo y sistemas de cómputo.

5) Las organizaciones deben de emprender un cambio hacia el control de seguridad apoyándose en sistemas administradores de accesos, ya que de no hacerlo estarán destinadas a perder campo dentro del medio económico en el que se encuentran.

9) Aumenta el número de organizaciones que experimentan problemas de seguridad, pero que no pueden contratar a más personas y adquirir los equipos y tecnologías necesarios para evitarlos por problemas de presupuesto. En general, muchas compañías no pueden o no quieren invertir en una estrategia de seguridad adecuada.

10) Las necesidades de rastreo en transacciones hechas por los sistemas de la organización, es una necesidad para conocer y atacar las inconsistencias de información. Este rastreo de transacciones, no se llevaba acabo, pero gracias a la implantación de éste sistema, como se explica en el capítulo II, se logró identificar varios elementos claves para proteger la base de datos.

11) Por si solo un sistema administrador de seguridad, no podrá delimitar todos los posibles fraudes o contingencias que pudieran surgir, para esto es necesario elaborar junto con el sistema informático, políticas de auditoria y seguridad informática.

12) Para el desarrollo de los diversos programas de seguridad es necesario basarse en una adecuada Administración de los riesgos. La administración de los riesgos es la identificación, evaluación y la posterior adopción de medidas que tiendan a minimizar y mantener los riesgos a un nivel aceptable para la organización

13) El tiempo es un factor determinante cuando se habla de innovación tecnológica pues se corre el riesgo de terminar un proyecto cuando sea obsoleto.

TESIS CON
FALLA DE ORIGEN

Bibliografía General

- Eric S. Raymond, "The New Hacker's Dictionary" Segunda Edición 1996
- Kendall & Kendall, "Análisis y Diseño de Sistemas", Prentice Hall 3ra Edición-1997
- William G. Page, Jr, "Oracle 8/8i" , Ed. Prentice Hall, Edición Especial 1999
- S.M. Deen. "Fundamentos de los sistemas de bases de datos", Ed. Gustavo Gili, S.A., Barcelona 1987
- Glenn A. Jackson "Introducción al Diseño de Base de Datos Relacionales" Ed. Prentice-Hall
- John G. Burch, Jr, Felix R. Strater Jr. "Sistemas de información Teoría y Práctica", Ed. Limusa 5ta Ed 1986
- C. West Churchman "El enfoque de sistemas para la toma de decisiones" Ed. Diana México 1973
- ACKOFF, Russel L., "El arte de resolver problemas", Ed. Limusa, México, 1981
- A.J. Thomas I.J. Douglas "Auditoría Informática" Ed. Paraninfo, Segunda Edición
- Yann Derrien "Técnicas de la auditoría informática" Ed. Alfaomega marcombo.
- S.M. Deen "Fundamento de los sistemas de bases de datos", Colección Ciencia Informática 1985.
- E. Yourdon, "Análisis Estructurado Moderno" Ed. Prentice Hall, 1994
- Sommerville, "Software Engineering" Ed. Addison-Wesley 1996
- John G. Burch, Jr "Sistema de información teoría y práctica" Ed. Limusa 1986.
- Perter Bishop "Conceptos de Informática" Ediciones Anaya Multimedia, S.A. 1989 Capitulo I
- Prof. Carlos A. Fernández y Fernández "Instituto de Electrónica y Computación", Universidad Tecnológica de la Mixteca (Apuntes)
- Díaz Gustavo, "Como operar el cambio vía reingeniería", Revista Acta Académica, Universidad Autónoma de Centro América, número 22, Mayo 1998
- Kendall &Kendall., Análisis y Diseño de Sistemas PrenticeHall Hipanoamericana, S.A. de C.V. 1997
- Hersey, Paul. "Estilo Eficaz De Dirigir : Liderazgo Situacional, No Existen Dos Situaciones Iguales / Paul Hersey Y Ken H. Blanchard. México, D.F. : Idh Ediciones, C1981.
- Dobyns, Lloyd. 1990. "Ed Deming wants big changes and he wants them fast." Smithsonian 21:

TESIS CON
FALLA DE ORIGEN