UNIVERSIDAD LASALLISTA BENAVENTE

ESCUELA DE INGENIERÍA EN COMPUTACIÓN CON ESTUDIOS INCORPORADOS A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

CLAVE: 8793-16

"SEGURIDAD EN EL ACCESO A LOS SISTEMAS DE INFORMACIÓN"

TESIS

QUE PARA OBTENER EL TÍTULO DE:

INGENIERA EN COMPUTACIÓN

PRESENTA:

TANIA GUADALUPE MARTÍNEZ AGUIRRE

ASESOR:

ING. ALEJANDRO GUZMÁN ZAZUETA

CELAYA, GTO. **DICIEMBRE DEL 2008**

AGRADECIMIENTOS

A mi Universidad y Catedráticos

A mi asesor de tesis

A mis Familia y Esposo

A mi hija Brenda
Eres el solecito que ilumina mi vida, te quiero mucho.

ÍNDICE GENERAL

INTRODUCCIÓN

CAPÍTULO PRIMERO

Conceptos Básicos

CAPÍTULO SEGUNDO

Seguridad Física

CAPÍTULO TERCERO

Seguridad Lógica

CAPÍTULO CUARTO

Políticas Y Diagnósticos De Seguridad

CAPÍTULO QUINTO

Ejemplo Práctico: Sistema De Inventario Para La Tienda De Ropa Y Accesorios Para Bebé "Periquita"

INTRODUCCIÓN

La seguridad en el acceso a los sistemas de información, es un tema muy importante, ya que hoy en día el mundo entero se rige y maneja por medio de estos, por lo que es de suma y vital importancia que dichos sistemas sean seguros, inalterables e inviolables por personas ajenas o malintencionadas.

En el mundo informático actual, existen muchas amenazas que pueden dañar la integridad de los sistemas de información, por lo que es muy importante protegerlos de manera física y lógica.

Este trabajo se compone de cinco capítulos a lo largo de los cuales se explicará: En el primer capítulo, el concepto de seguridad en los sistemas de información y la importancia de este concepto en el mundo actual que repercutirá en las ganancias o pérdidas de las empresas básicamente. En el segundo capítulo se describirán las medidas de control físico que se deben tomar para evitar el acceso no autorizado a los espacios físicos donde reside el hardware que utiliza el sistema o los sistemas de información. El tercer capítulo trata de los métodos lógicos que se utilizan para la seguridad informática. El cuarto capítulo explica la importancia de la existencia de políticas de seguridad en una empresa, así como también de la necesidad de hacer diagnósticos al sistema de seguridad y al sistema de información con el fin de detectar malfuncionamientos o falta de seguridad en alguno de ellos. Y por ultimo en el quinto capítulo se expondrá un ejemplo de un sistema de información que aplicará los conceptos vistos en los anteriores cuatro capítulos.

CAPÍTULO PRIMERO: *Conceptos Básicos*

En este capítulo se dejará claro el concepto de sistemas de información, se definirá también la seguridad en estos, así como el impacto negativo de la ausencia de seguridad en los sistemas de información.

Es importante comenzar con una pequeña definición de sistemas de información.

Un sistema de información es un medio por el cual los datos fluyen de una persona, departamento o equipo de cómputo a otro y están compuestos básicamente por una base de datos y un manejador de base de datos.

Las finalidades de los sistemas de información dentro de una empresa, son procesar entradas, conservar la información y producir información, reportes y otras salidas. [1]

[1] Senn, James A., **Análisis y diseño de sistemas de información**, Segunda edición, Ed. McGraw-Hill, Colombia, 2000, Pags. 20,23.

1.1 Importancia de un sistema de información

Para que un sistema de información sea funcional, debe de cumplir con los siguientes objetivos:

- **Resolver un problema.** Las actividades, procesos o funciones que no cumplen con las necesidades de la empresa.

- **Mejorar el rendimiento.** Los sistemas se pueden utilizar para mejorar el rendimiento de la empresa y hacerla más competitiva en el mercado.

- **Dar respuestas a directivos.** Proporcionar la información solicitada por los directivos de una manera organizada y correcta, que ayudará a estos en la toma de decisiones.

Para cumplir estos objetivos se deben de tomar en cuenta cinco puntos importantes que se describen en los siguientes incisos:

a) **Capacidad**. Las actividades de una empresa están influenciadas por la capacidad de dicha empresa para procesar transacciones con rapidez y eficiencia. Los sistemas de información mejoran esta capacidad en tres formas: [2]

[2] http://www.monografias.com/trabajos14/proyectos-sistem/proyectos-sistem.shtml

1. Aumentar la velocidad de procesamiento. El uso de la computadora en el proceso de datos reduce el tiempo de ejecución notablemente.
2. Permitir el manejo de un volumen creciente de transacciones. El uso de la computadora, permite manejar grandes cantidades de información.
3. Recuperar con fluidez la información. Las empresas almacenan grandes cantidades de datos relacionados con sus operaciones, empleados, clientes, proveedores y finanzas, por lo que el uso de la computadora permitirá al usuario tener acceso más rápido a la información que está buscando que por ejemplo en un archivero, ya que esta información se encuentra organizada.

b) **Comunicación.** La falta de comunicación es una fuente común de dificultades que afectan las relaciones cliente-proveedor. Un sistema de información resuelve este problema. [3]

1. Aumento de la comunicación. Muchas empresas aumentan sus vías de comunicación por medio del desarrollo de redes especiales para este fin.
2. Integrar áreas de la empresa. Con frecuencia las actividades de las empresas abarcan varias áreas de la organización; el trabajo realizado en un área se confunde con el que se efectúa

[3] http://www.monografias.com/trabajos14/proyectos-sistem/proyectos-sistem.shtml

en otro lugar. Para coordinar mejor las operaciones, la administración contribuye con la implantación de terminales con sistemas de información operativos entre los departamentos de producción y compras de donde se extraen reportes de ambos lados con datos como los inventarios disponibles para producción y los requerimientos de las compras de materiales.

c) **Costo.** Muchas empresas han quedado fuera de la actividad comercial y otras imposibilitadas para alcanzar el éxito por el poco control sobre los costos o por el total desconocimiento de estos. Los sistemas de información juegan un papel muy importante tanto en la vigilancia como en la reducción de costos de operación. [4]

1. Vigilancia de los costos. Llevar a cabo el seguimiento de los costos de mano de obra, bienes y gastos generales es un tarea esencial para determinar si la empresa evoluciona en la forma esperada, es decir de acuerdo a lo presupuestado.

2. Reducción de costos. Algunos diseños de sistemas ayudan a disminuir los costos ya que toman ventaja de la capacidad de cálculo automático y de recuperación de datos que están incluidos en los procedimientos de programas de computadoras.

d) **Control.** El controlar toda la información de la empresa de una manera segura, le da a la empresa mayor confianza en sus

[4] http://www.monografias.com/trabajos14/proyectos-sistem/proyectos-sistem.shtml

transacciones; esto se logra con la ayuda de la computadora por dos razones: [5]

1. Se mejora la exactitud. Dado que el sistema automatizará todos los procedimientos, se evitan en gran medida errores humanos.

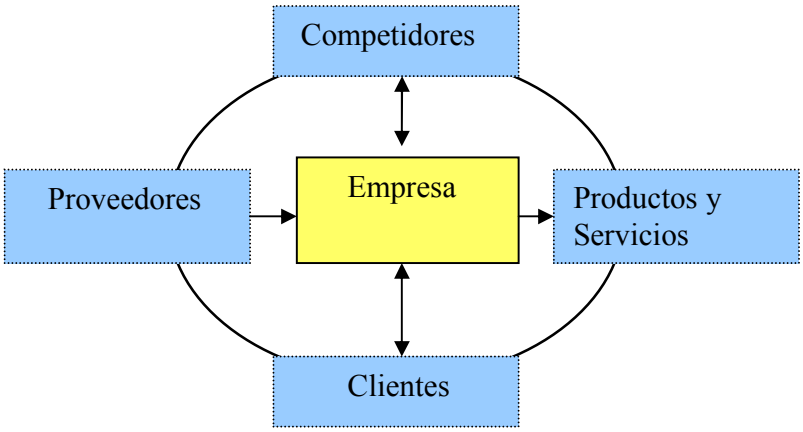
2. Aumenta la seguridad de los datos importantes. Algunas veces el solo hecho de que los datos sean guardados de una forma adecuada para su lectura por un equipo de cómputo, proporciona mayor seguridad que es difícil de alcanzar por un medio ambiente donde no se usa la computadora.

e) **Competitividad.** Los sistemas de información computacionales son un arma estratégica que puede cambiar la forma en que la empresa compite en el mercado. Como consecuencia de lo anterior, estos sistemas mejoran la organización y le ayudan a ganar ventajas competitivas. Por el contrario si los competidores de la empresa tienen capacidades más avanzadas para el procesamiento de información, entonces los sistemas de información pueden convertirse en una desventaja competitiva. Por lo tanto, las capacidades de los sistemas de información son una consideración importante al formular la estrategia de la empresa. Una organización puede ganar ventajas competitivas a través de sus sistemas de información por medio de 4 formas diferentes, donde cada una considera las entidades con las que la empresa trata como parte de

[5] http://www.monografias.com/trabajos14/proyectos-sistem/proyectos-sistem.shtml

sus actividades comerciales, estas son: 1. Clientes, 2. Competidores, 3. Proveedores y 4. Productos y servicios. [6]

Fig. 1.1 Circulo de la competitividad[7]



1. Asegurar clientes. Ya que los clientes son lo más importante para una empresa, los directivos buscan formas diversas para acercarse a nuevos clientes y al mismo tiempo, retener los que tienen.

   ¿Cómo es que pueden los sistemas de información de la compañía ofrecer en este caso una ventaja competitiva o un beneficio significativo sobre sus competidores? Pues ofreciendo mejores servicios y proporcionando servicios exclusivos.

[6] http://www.monografias.com/trabajos14/proyectos-sistem/proyectos-sistem.shtml
[7] http://www.monografias.com/trabajos14/proyectos-sistem/proyectos-sistem.shtml

2. Dejar fuera a los competidores. Dar el salto sobre los competidores puede ser riesgoso si ellos encuentran la forma de duplicar los logros de la compañía. Los descuentos como ejemplo no brindan beneficios estratégicos a largo plazo, sin embargo los sistemas de información pueden ser la base para dejar fuera del mercado a la competencia, ya sea al disuadir sus intentos por ingresar al mercado o creándoles obstáculos para su entrada.

3. Mejores acuerdos con los proveedores. En los negocios los proveedores también tienen importancia estratégica. Una manera de utilizar los sistemas de información para favorecer arreglos con los proveedores es recibiendo un mejor precio, pronosticando inventarios con un sistema de abastecimiento anual generado a través de reportes de consumo estadístico de los pedidos a los proveedores o pedidos por Internet.

4. Formar bases para nuevos productos. Los sistemas de información también forman la base para la creación, promoción y distribución de nuevos productos y servicios.

Como se ha visto, el uso de un sistema de información computacional es muy importante para el desarrollo y buen funcionamiento de una organización, y para asegurarnos que dicho sistema funcione correctamente y no sea victima de ataques es muy importante implantar un buen sistema de **seguridad** en dicho sistema.

Hoy en día todo se maneja por medio de la computadora, es decir, todas las decisiones importantes de una empresa se toman a partir de los reportes que arroja un sistema después de procesar los datos, y si estos datos o reportes llegan a ser falsificados y/o manipulados incorrectamente, la empresa sea del tipo que sea no tendrá un funcionamiento adecuado.

1.2 Seguridad en los Sistemas de Información

Para poder decir que un sistema de información es seguro debe de cumplir básicamente con los siguientes puntos:

- **La confidencialidad en la información.** Es restringir el acceso a la información, de tal forma que solo las personas, procesos o entidades autorizadas pueden tener derecho a ver, tal o cual información.

- **Integridad en la información**. Tener un sistema íntegro, significa que la información de dicho sistema solo pueda ser modificada incluyendo su creación o destrucción, por las personas designadas o responsables de esta tarea.

- **Accesibilidad en la información.** Es tener un control a cerca de las personas que tienen acceso a la información, es decir, permitir o no permitir, el acceso a la información dependiendo si tal o cual persona está autorizada para poder ver esta información.

- **Conservación de la información.** Un sistema de información debe de ser capaz de almacenar la información correctamente y realizar los procesos sin fallas o errores. Esto se logra haciendo una buena planeación y programación del sistema.

1.2.1 ¿Qué es la seguridad en el acceso a los Sistemas de Información?

Seguridad o sistemas de seguridad en el acceso a los sistemas de información, es el conjunto de reglas programadas que existen en un sistema de información, y que cumplen con los cuatro puntos que se mencionaron en el tema anterior y con los siguientes:

Que sea **disponible**, es decir, que los datos puedan accederse en el momento en que el personal autorizado lo requiera.

Que sea **confiable**, es decir, que el hardware que se usa para operar el Sistema de información sea de buena calidad, y que el sistema de información tenga el mínimo de errores.

1.2.2 Medidas importantes de seguridad en el acceso a los Sistemas de Información

Las funciones, servicios y mecanismos de seguridad de una empresa requieren, en general, la combinación de una serie de medidas que se pueden clasificar como:[8]

[8] http://www.csi.map.es/csi/silice/Segurd4.html

- **Medidas administrativas u organizativas de los sistemas.** Deben definirse claramente las áreas de responsabilidad de usuarios, administradores y directivos.

- **Medidas legislativas.** En los casos en que la prevención no sea técnicamente posible, deben preverse acciones penales a las personas que hagan mal uso de sus concesiones de acceso al sistema de información.

- **Medidas técnicas**
  - Encriptar documentos
  - Recuperación de ficheros dañados
  - Copias de seguridad
  - Identificación y autenticación de usuarios

1.2.3 Factores importantes para determinar el Sistema de Seguridad óptimo para una empresa

El sistema de seguridad requerido por un sistema de información o una organización para prevenir el acceso no autorizado, variará dependiendo de una serie de factores, entre los que pueden destacarse los siguientes: [9]

[9] http://www.csi.map.es/csi/silice/Segurd4.html

- **Localización geográfica de los usuarios.** Cuando el sistema solo se maneja en un espacio físico especifico (Por ejemplo cuando en sistema reside en una sola maquina o en una Red de Área Local), la seguridad en esté será menor que la que se necesita si el sistema puede ser accesado por usuarios que se encuentren en espacios físicos distintos.

- **Instalaciones o salas donde residen los equipos físicos.** El equipo físico debe residir en espacios asegurados con puertas y ventanas difícilmente violables, si no es así deben aplicarse otras medidas de seguridad como guardias y cámaras que minimicen el riesgo de acceso a los sistemas.

- **Equipo físico que soporta el sistema de información.** Los equipos de cómputo que contengan los sistemas de información deben estar en buen estado y tener la capacidad suficiente para soportarlos.

- **Diseño de las bases de datos.** Para implanta un adecuado control de acceso al sistema de información, se bebe de conocer el diseño de la base de datos del mismo.

- **Tipo y cantidad de información que maneja el sistema.** El nivel de seguridad en el acceso a los sistemas de información está directamente relacionado con la cantidad de información que se maneja y el nivel de confidencialidad en el mismo. A mayor

necesidad de confidencialidad y mayor cantidad de datos a procesar, mayor será el nivel de seguridad requerido.

Entonces se dice que: Seguridad en el acceso a los sistemas de información es tener medidas de control en el sistema muy restringidas y personales, de tal forma que solo las personas autorizadas y capacitadas para acceder sean las que puedan entrar.

1.3 Riesgos de Seguridad

Es muy importante tener bien definidos o ubicados todos los riesgos de seguridad que puede sufrir un sistema de información especifico, ya que esto nos permitirá realizar un buen sistema de seguridad en el sistema de información.

Los elementos de seguridad que se deben de considerar son: activos, amenazas, vulnerabilidades, impactos, riesgos y defensas, cada uno de los cuales se explica en los siguientes puntos.[10]

- **Activos:** Se definen como los recursos del sistema de información necesarios para que la empresa funcione de manera adecuada. Los activos serian: La instalación física, el sistema de información, la información.

[10] http://www.csi.map.es/csi/silice/Segurd7.html

- **Amenazas:** Se define como las situaciones que pueden desencadenar un problema en la empresa, produciendo daños materiales o pérdidas inmateriales en sus activos.
- **Vulnerabilidad:** Cualquier debilidad en el sistema de información que pueda permitir a las amenazas dañar el sistema.

- **Impacto:** Es el resultado de la agresión sobre el activo. Se pueden clasificar los impactos sobre los activos a partir de sus consecuencias como:
    - Cuantitativo. Representa pérdidas en dinero ya sea directa o indirectamente.
    - Cualitativo con pérdidas orgánicas. Representa daño de personas.
    - Cualitativo con pérdidas funcionales. Representa daños a los sistemas de seguridad.

- **Riesgo:** Se define como la posibilidad de que exista un impacto dañino en la organización.

- **Defensas:** Cualquier medio físico o lógico utilizado para eliminar o reducir un riesgo.

1.4 Tendencias Actuales

Para tener un efectivo sistema de seguridad en los sistemas de información es necesario tener en cuenta las tendencias actuales, es decir, saber que ahora se están manejando muchos sistemas por medio de redes lo que obliga a tener mayor control en todo lo referente a acceso, y también es importante destacar que ahora los equipos cuentan con tecnologías que años atrás no existían, y que podemos hacer buen uso de estas herramientas.

El incremento de las empresas que se comunican por medio de redes, se debe a que en la actualidad los sistemas tienden a estar descentralizados, es decir, que el mismo sistema puede ser usado por los diferentes departamentos de una empresa, aunque esta necesariamente no esté en la misma ubicación geográfica, o en el caso de páginas de Internet, por cualquier usuario.

Pongamos un ejemplo, para que al lector le quede más claro el concepto: Supongamos que existe una empresa llamada “Pollos nuevos”; esta empresa se dedica a vender pollos crudos y tiene sucursales en diferentes estados de la Republica Mexicana con una sucursal matriz en la ciudad de Monterrey.

Todas las sucursales usan el mismo sistema de información, es decir que la información de toda la organización se encuentra en una misma base de datos, razón por la cual, es muy importante que esta organización tenga implementado un buen sistema de seguridad, que restrinja los accesos a la información de manera que solo las personas autorizadas pueden consultarla.

Con el uso de redes es necesario, incrementar el nivel de seguridad de los sistemas operativos en la concesión de permisos de acceso, la protección de ficheros individuales, la evaluación del historial de seguridad del usuario, la evaluación del historial de los datos. Todo esto implica un considerable esfuerzo en la creación de un sistema de seguridad, que puede incluir desde contraseñas simples hasta tarjetas inteligentes para el control de accesos a datos o instalaciones.

El uso cada vez más extendido de comunicaciones electrónicas a larga distancia, donde además de voz y datos simples, se transfieren documentos mercantiles, dinero, etc., provoca una demanda de equipos que proporcionen autentificación de mensajes y firma digital, reconocimiento de voz, etc.

Este trabajo sin embargo, no profundizará en la seguridad en redes.

CAPÍTULO SEGUNDO: *Seguridad Física*

En este capítulo, se explicará todo lo referente a la seguridad física en el acceso a los sistemas de información, ¿Qué es la seguridad física en el acceso a los sistemas de información?, cómo implementarla, así como la importancia de tener un buen sistema de seguridad física para garantizar la integridad del sistema de información.

La seguridad física consiste básicamente en la protección de todo el Hardware que utiliza el sistema de información. Por ejemplo la protección de las computadoras, de copias de respaldo, etc.

La seguridad física de los sistemas de información consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención contra las amenazas a los recursos y la información confidencial. Estos recursos son desde un simple teclado hasta una cinta de respaldo con toda la información que contiene el sistema.

El equipo físico, debe de estar asegurado de tal forma que se necesite una apropiada identificación para poder entrar al lugar donde se encuentra, así como también el espacio físico donde se encuentre el equipo, deberá de estar acondicionado adecuadamente.

El acceso físico al sistema puede crear muchos problemas de seguridad por diferentes razones. Muchas herramientas son utilizadas para extraer contraseñas e información de cuentas, y esta información a su vez, usada para tener acceso a información privada del sistema.

Aunque la seguridad física incluye también la prevención de daños en el equipo físico (Computadoras, Discos, etc.) causados por inundaciones, incendios entre muchos otros, este trabajo solo abarcará la seguridad física para prevenir el acceso no autorizado al hardware que maneja o contiene el sistema de información.

2.1 Control de acceso

Cuando la seguridad física es examinada, la consideración más obvia, es el control del acceso físico al sistema o a los recursos. La meta es permitir solo el uso de estos recursos a personas debidamente identificadas. Para que esta meta se cumpla deben aplicarse las siguientes normas:

- **Cerrar las instalaciones donde reside el equipo físico**. Se debe tener el cerrojo más seguro en las puertas y ventanas, además asegurarse que no se pueda entrar a las instalaciones por los conductos de aire acondicionado, el techo o el piso. Esta es la medida de seguridad física básica para prevenir el acceso no autorizado a los dispositivos.

Las siguientes normas de seguridad física a diferencia de la anterior, se aplicarán dependiendo el nivel de confidencialidad y cantidad de información que maneje el sistema de seguridad a proteger.

- **Guardias de seguridad.**
- **Cámaras de seguridad.**
- **Detectores de movimiento.**
- **Zonas de acceso limitado y acceso biométrico.** Para áreas restringidas pueden ser consideradas cuando se planee el control de acceso.

Y para terminar se debe de educar a los usuarios para que reporten cualquier anomalía.

2.1.1 Ingeniería social

Dentro del control de acceso se debe prever el fenómeno de la ingeniería social que es el proceso por el cual un atacante extrae información valiosa de los usuarios por medio de engaños.

Ejemplos comunes de ataques con ingeniería social incluyen lo siguiente:

- Un atacante contacta a un usuario válido pretendiendo ser un invitado o un nuevo usuario preguntando por asistencia para accesar al sistema o detalles del proceso de negocios de la organización.

- El atacante contacta a un usuario legítimo fingiendo ser un ayudante técnico intentando dar de alta algún tipo de información y pregunta por los detalles de identificación de un usuario y esta información puede ser usada para conseguir el acceso.

- El atacante finge ser un administrador del sistema y pide a un usuario legitimo modificar sus códigos de acceso con un valor específico para luego poder usarlo y accesar al sistema.

Dentro de la ingeniería social, se encuentra la ingeniería social a la inversa donde el atacante provee información verdadera al usuario para que éste lo crea un técnico autorizado y entonces le proporcione toda la información que ahora el atacante le pedirá.

Para prevenir la ingeniería social y la ingeniería social inversa, los usuarios no deben proporcionar información privada a personas no identificadas propia y ampliamente.

Es importante prevenir a todos los usuarios del sistema de la existencia de este tipo de ataque para que no los tome por sorpresa y sean presa fácil de este tipo de atacantes.

2.2 Ambiente

El control del ambiente en la seguridad física incluye la prevención contra terremotos, inundaciones, problemas eléctricos, incendios y la protección de los datos. No obstante, este trabajo solo incluirá la protección de los datos ya que los otros puntos no están relacionados con el acceso a los sistemas de información.

En corporaciones ya muy grandes la colocación de todas las cosas en un edificio actual con antenas inalámbricas afecta la seguridad. Cuando se escoja la colocación de un edificio, una organización debe de investigar el tipo de vecindario, población, cantidad de crimen, y el tiempo de respuesta a una emergencia, esto puede ayudar para determinar el tipo de barreras que se necesitan como cercas, alumbrado, personal de seguridad.

2.2.1 Protección de los datos

La seguridad física también implica una protección a la información del sistema, tanto a la que está almacenada en él (Backup) como a la que se transmite entre diferentes equipos (Passive Wiretapping).

2.2.1.1 Backup (Copias de seguridad)

Las copias de seguridad son copias del sistema que se realizan periódicamente para evitar pérdidas de información en caso de problemas con el hardware o el software.

Los siguientes son los diferentes tipos de respaldos que existen:

- Respaldo completo. Este respaldo contiene todos los datos, y es la forma de respaldo más intensiva en tiempo y en recursos.

- Respaldo diferencial. Un respaldo diferencial incluye todos los datos que han cambiado desde el último respaldo completo.

- Respaldo copia. Un respaldo copia es muy parecido al respaldo total, en este respaldo se copian todos los archivos seleccionados.

Para minimizar el riego de robo, las copias de seguridad deben de estar guardadas en un ambiente seguro, además, asegurarse que los empleados que no están a cargo de hacer los respaldos no conozcan el

lugar donde están guardados los respaldos. En una empresa pequeña con guardar las copias de seguridad en un lugar contra incendios y completamente cerrados es suficiente, en cambio en una organización grande es conveniente mover las copias de lugar cada cierto tiempo.

2.2.1.2 Passive Wiretapping (Interceptores pasivos de la información que fluye a través de la red)

Este peligro es cuando nuestro sistema es un sistema en red. Un intruso capta la información que fluye a través de la red por el medio del llamado spoofing que básicamente es una forma de hacer que la información sea enviada a una máquina intrusa, para poderla robar y utilizarla después en beneficio del intruso.

Para evitar la salida de información por este medio se deben de utilizar métodos de cifrado de datos que serán explicados más adelante.

Aparte del control de acceso y el ambiente, otras medidas de seguridad física son el no hablar de asuntos privados del sistema delante de personas no autorizadas o de lugares no seguros (Donde puedan estar siendo video grabados o grabados sin saber), ya que lo que se diga, podrá ser utilizado por el atacante para corromper el sistema.

CAPÍTULO TERCERO*: Seguridad Lógica*

En este capítulo se tratará todo lo referente a la seguridad lógica necesaria para prevenir el acceso no autorizado a los sistemas de información, ¿Qué es la seguridad lógica?, la importancia de ésta, así como todas las formas para implementar la seguridad lógica en los sistemas de información.

La seguridad lógica se refiere básicamente a la protección del sistema de información a nivel software. Por ejemplo el uso de contraseñas, antivirus, etc.

El objetivo de la seguridad lógica es proteger los activos de información de la empresa, aplicando barreras que eviten el acceso no autorizado a los datos de la misma y así evitar acciones que puedan provocar su alteración, borrado o divulgación no autorizados, de forma accidental o intencionada.

Los usuarios tienen que saber que el sistema solo puede ser usado para los fines de la propia empresa, y que el uso no autorizado del sistema es una violación a las políticas de la empresa y que merecerá una sanción.

3.1 Identificación de usuarios

El sistema debe tener un método de identificación de usuarios que contenga los siguientes elementos:

1. Identificador de usuario
2. Identificador de usuario compartido
3. Autorización de usuarios
4. Eliminación de usuarios
5. Revalidación anual de usuarios

1. **Identificador de usuario.** Es una clave que permite a un usuario en particular tener acceso al sistema de información de forma individual. Cada identificador de usuario tiene que estar asignado a

una persona, que debe de estar conciente que todas las actividades que se realicen con este son su responsabilidad.

Generalmente un identificador de usuario (Junto con el o los métodos de autenticación usados) se asigna a una persona para facilitarle el acceso a un sistema de Información único; entonces si la empresa maneja más de un sistema el usuario debe tener un identificador (Junto con el o los métodos de autenticación usados) por cada sistema. Esto provoca la multiplicidad de identificadores y autenticadores que tendrá que conocer el usuario.

Para evitar este posible problema, se recomienda:

- Definir y utilizar una nomenclatura estándar en la creación de identificadores, de tal forma que un usuario tenga el mismo identificador en todos los sistemas que necesite utilizar.

- Tener un sistema de control de accesos que gestione todos los sistemas de Información de la empresa, para que el usuario utilice un único identificador en los sistemas de la misma.

- Utilizar un método de identificación única, que permita al usuario en su primera conexión a los sistemas, realizar el proceso de identificación y autenticación, pudiendo posteriormente tener acceso a cualquier otro sistema o servicio de la empresa.

Cuando la empresa maneja varios sistemas de información, en cada uno de los cuales es necesaria la identificación y

autentificación de usuario, es recomendable dedicar un sistema a las funciones de control de seguridad, de tal forma que antes de permitir que un usuario tenga acceso a cualquier sistema de información de la empresa, se verifique primero y por única vez su identidad y autorizaciones de acceso.

2. **Identificador de Usuario Compartido.** Cuando un identificador de usuario permite el acceso a determinadas funciones del sistema (Por ejemplo Introducir datos) que tienen que ser utilizadas por un grupo de personas, se puede utilizar un identificador de usuario compartido para evitar asignar a cada miembro del grupo un identificador único.

   El identificador de usuario compartido debe de cumplir con los siguientes puntos:

   - El identificador de usuario compartido debe de ser creado para el uso del grupo, con sus restricciones y permisos, para manipular los datos; no puede contener información individual que el resto del grupo no deben conocer.

   - La contraseña no debe de ser compartida, es decir cada miembro de grupo tendrá que tener su propia contraseña.

3. **Autorización de Usuarios.** El permiso de acceso para cada nuevo usuario de los sistemas de la empresa tiene que primeramente ser

aprobado por la dirección o por la persona autorizada para otorgar permisos.

Se tiene que haber definido un procedimiento, automático o manual, para autorizar que se agreguen nuevos identificadores de usuarios en los sistemas y que incluya la notificación al responsable del usuario.

4. **Eliminación de Usuarios.** En caso de tener que eliminar a un usuario del sistema, tiene que haber definido un procedimiento, automático o manual, para la eliminación de identificadores de usuarios del sistema.

   El procedimiento debe incluir los controles para prevenir el acceso de un usuario a los sistemas, inmediatamente después de haber dejado de pertenecer a la empresa. Un identificador de usuario eliminado, no volverá a ser asignado a ningún otro usuario de sistema.

   Dentro de este procedimiento se encuentran la revisión de vigencia y la identificación de usuarios inactivos.

Revisión de vigencia. Para evitar que existan identificadores de usuario no vigentes, es decir los pertenecientes a usuarios dados de baja en la empresa, tiene que haber un proceso periódico de revisión de identificadores.

Este proceso puede utilizar como base la comparación con listas de empleados actualizadas y servirá de proceso de corrección en los

casos en que el procedimiento de eliminación de usuarios no haya sido aplicado correctamente.

Todos los identificadores de usuario de los empleados dados de baja en la empresa encontrados en este proceso tendrán que ser eliminados del sistema, junto con todos los derechos de acceso concedidos, y su baja debe ser comunicada al responsable del empleado.

Usuarios Inactivos. El acceso no autorizado a un sistema se puede dar através de un identificador de usuario inactivo, por lo que es recomendable utilizar controles que detecten identificadores de usuario que no se hayan usado en los últimos seis meses.

El proceso para detectar a los usuarios inactivos, debe realizarse a menos cada mes, y una vez detectados este tipo de usuarios, desactivar su acceso al sistema.

La desactivación del acceso debe ser comunicada al responsable del empleado.

5. **Revalidación anual de usuarios.** Cada año, es recomendable hacer una revalidación de usuarios, es decir, verificar si todos los usuarios activos en el sistema aun pertenecen a la empresa y conservan sus derechos de acceso.

   Esta revalidación se hace por medio de un procedimiento que consiste en enviar la relación de usuarios a cada director que tiene empleados trabajando en el sistema, para que confirme si todos y cada uno ellos siguen siendo empleados de la empresa y si

conservan sus derechos de acceso al sistema. Las anomalías deben ser comunicadas a la administración de seguridad para poder desactivar o eliminar a los usuarios.

3.2 Autenticación de usuarios

La autenticación de usuarios permite al sistema comprobar que la persona que quiere tener acceso a el es quien dice ser.

La autenticación de usuarios puede ser por uno o varios de los siguientes métodos:

1. Contraseñas.
2. Tarjeta, dispositivos, etc.
3. Características biométricas

La utilización de sólo uno de los métodos de autenticación anteriores es llamada autenticación simple.

Aunque la mayoría de los sistemas de información utilizan la autenticación simple por contraseña, cuando los controles de acceso tienen que ser muy restrictivos, pueden combinarse dos o más métodos de autenticación para eliminar, o al menos reducir, los riesgos de que sea utilizado un identificador sin autorización. En este caso se le llama autenticación reforzada.

1. **Contraseñas.** El uso de contraseñas para la autenticación del usuario es la opción de protección más usada hoy en día, ya que

permite verificar sin equivocación la identidad del usuario del sistema.

La contraseña debe de considerarse información privada y muy importante para la seguridad del sistema. Por lo que la contraseña debe de cumplir con los siguientes puntos:

- Tiene que ser secreta e individual, es decir. no compartirla con nadie.

- No puede visualizarse en pantalla mientras se esta tecleando.

- Tiene que ser cifrada para ser almacenada en el sistema.

La contraseña debe tener las siguientes características de calidad para que sea segura: [11]

- Tener una longitud mínima de ocho caracteres, 14 caracteres es lo ideal.

- Combinar letras números y símbolos, teniendo en cuenta que a menor tipo de caracteres mas larga tiene que ser la contraseña.

✓ [11] http://www.microsoft.com/latam/athome/security/privacy/password.mspx

- No tener más de dos caracteres iguales consecutivos.

- Utilizar mayúsculas y minúsculas.

- Debe ser cambiada cada sesenta días para usuarios generales, y cada treinta días para usuarios que tengan algún privilegio o autoridad. Se debe de tener un control programado que informe a los usuarios cuando su contraseña debe de ser cambiada.

- La contraseña no debe de ser reutilizada, y si lo hace al menos debe de esperar doce cambios.

- No utilizar el identificador de usuario como parte de la contraseña.

La contraseña que en muchos casos los sistemas operativos, productos informáticos o aplicaciones traen por defecto para ser usada durante su instalación, debe de ser cambiada lo más pronto posible.

Si por razones de negocio, un usuario tiene que utilizar sistemas no pertenecientes a la empresa, deberá utilizar una contraseña diferente a la utilizada en los sistemas internos de la empresa, ya que podría ser detectada y utilizada de manera inadecuada en los sistemas de la empresa.

Restauración de contraseñas. Se debe tener un proceso para asegurar la restauración o cambio de contraseña por pérdida u olvido de la anterior o cuando se sospeche que es conocida por otra persona. El proceso debe incluir la identificación del usuario, y en caso de que la identificación del usuario no sea correcta, enviar la nueva contraseña al jefe del solicitante.

La solicitud de nueva contraseña y la respuesta deberán realizarse através de medios seguros.

Contraseñas de un solo uso. Las contraseñas de un solo uso son como su nombre lo indica contraseñas que solo se pueden utilizar una sola vez, de tal modo que los datos de acceso estuvieran caducados cuando se trate de accesar nuevamente.

La contraseña de un solo uso consiste en un generador de contraseñas (dispositivo físico o lógico) interno o externo al sistema, al que quiere conectarse el usuario.

2. **Tarjetas, dispositivos, etc.** Son dispositivos que contienen una clave única para cada usuario y que permite su identificación inequívoca. Un ejemplo son las tarjetas de crédito o débito que traen una clave.

3. **Identificación biométrica.** Esto se refiere a un dispositivo conectado al sistema que identifica alguna parte de nuestro cuerpo, por ejemplo el pulgar, el rostro, la voz. Este tipo de identificación se

usa cuando el sistema al que se desea acceder es sumamente privado.

3.3 Activos de información del sistema

A todos los recursos del sistema de información o relacionado con éste (datos, programas, subsistemas, etc.), necesarios para que la organización funcione correctamente, se denominan activos de información del sistema. [12]

Los activos de información deben protegerse para asegurar su integridad.

Entre los activos de la información del sistema cabe definir o destacar:

- Los programas de control del sistema y sus mecanismos de control de acceso.

- Los subsistemas, y productos soportados por sistemas de información, que formen parte del sistema operativo y sus funciones.

- Las bases de datos donde se almacena la información del sistema.

[12] http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

3.3.1 Activos sensibles del sistema

Los activos sensibles del sistema, son los datos y programas que por su importancia para el buen funcionamiento de los sistemas son calificados como sensibles por el departamento de sistemas.

Un dato sensible es cualquier activo de información del sistema que al ser modificado o utilizado inadecuadamente de manera accidental o malintencionada, puede afectar gravemente a la integridad y el buen funcionamiento del sistema de información.

Es importante destacar que, este tipo de Activos tienen que ser actualizados a través de un programa o transacción del propio sistema y nunca pueden ser modificados o actualizados directamente. (Ejemplo: los activos que contengan las contraseñas de acceso al sistema).

Un programa sensible es cualquier programa de utilidad o del sistema mismo, cuyo uso no autorizado o inadecuado de manera accidental o malintencionada, puede poner en riesgo la integridad y el buen funcionamiento del sistema de información. También es considerado sensible cualquier programa de utilidad o del sistema, que actualice activos de información definidos como datos sensibles. (Ejemplo: cualquier utilidad del sistema que actualice los grupos de usuario en un sistema).

Es importante destacar que los activos sensibles del sistema no deben ser accesados públicamente, es decir que solo los usuarios que se identifiquen adecuadamente puedan accesar a estos activos y que no debe haber usuarios permanentes de este tipo de activos.

Cuando se necesite tener acceso a los activos sensibles del sistema, se debe de justificar plenamente la necesidad de acceso y se tendrán que registrar y analizar todas las actividades que realice el usuario mientras tenga acceso a dichos activos.

Los accesos temporales tendrán que ser eliminados inmediatamente después de que el usuario termine de realizar los trabajos para los cuales fue necesario el acceso a los activos sensibles del sistema.

3.4 Activos de información de usuario

Los activos de información de usuario son los activos de información que pertenecen a un usuario o a un grupo de usuarios, a una aplicación o son parte de alguna de ellas.

El propietario del activo de información de usuario, tiene la responsabilidad de establecer la protección del activo, teniendo en cuenta los riesgos a los que queda expuesto éste si ni se protege adecuadamente.

El propietario tendrá que asegurarse de que los activos de información de usuario permanezcan íntegros.

Se debe de asegurar que cada activo de información de usuario esta protegido, y que solo tienen acceso a este las personas autorizadas.

Perfiles de Usuario: En los sistemas de información cada usuario tiene acceso solo a los datos que necesita para desempeñar sus funciones dentro de la organización, es decir, se crean perfiles de cada tipo de

usuario para asignarle los permisos de acceso a las partes del sistema que este necesita para desempeñar sus funciones .

Es importante definir también dentro del mismo perfil hasta que punto dicho usuario puede manipular los datos a los que tiene acceso, es decir, si dicho usuario solo puede consultar datos (Nivel mas bajo dentro del mismo perfil); consultar e ingresar datos (Nivel intermedio dentro del mismo perfil); y consultar, ingresar y modificar datos (nivel mas alto dentro del mismo perfil).

3.4.1 Control de Acceso Público

Los activos de información de usuario no deben tener ninguna opción que permita su acceso público (Ejemplo: Los sistemas de información que pueden ser accesados por medio de internet, deben establecer mecanismos de seguridad para que solo el personal autorizado pueda accesar e ellos).

Si un usuario considera que alguno de sus activos tiene que ser de acceso público, debe:

- Asegurarse que el activo no tiene información clasificada.

- Comunicar que va a hacer su acceso público al departamento de sistemas de información.

- El departamento de sistemas de información, evaluará la propuesta y si es aceptada lo anotará en su lista de excepciones autorizadas y

le notificará al propietario que su activo va a ser de acceso público, esto es, que podrá ser accesado por todos los usuarios del sistema incluyendo usuarios externos.

Revisión periódica. Los sistemas de información deben tener una función que compare, al menos, mensualmente los activos de información de usuario que pueden ser accesados públicamente con la lista de excepciones autorizadas o si no se tiene aun esta aplicación hacerlo manualmente.

Si durante esta comparación se encuentra algún activo de información de usuario con acceso público y no registrado, se restaurará la protección inicial por defecto permitiendo su acceso sólo al propietario.

3.4.2 Activos sensibles de usuario

Los activos sensibles de usuario son los datos y programas que son clasificados por el propietario como sensibles.

Un dato sensible es cualquier activo de información que si es modificado o eliminado malintencionadamente, puede causar perdidas financiaras graves a la empresa y problemas muy serios al usuario involucrado. La modificación de estos datos sensibles no puede ser detectada en un espacio corto de tiempo y tampoco prevenidas fácilmente. Un ejemplo de este tipo de activos es la información de los pagos a los empleados.

Un programa sensible es cualquier programa de aplicación que si es modificado de manera inadecuada o no autorizada, puede causar graves pérdidas financieras a la empresa que no pueden ser detectadas ni prevenidas por los métodos habituales de control.

Un programa sensible es también cualquier programa de aplicación que actualice activos de información definidos como datos sensibles.

Cuando un programa sensible sufra alguna modificación, cambio o alteración ordenada por el propietario, un programador independiente del que realizo la modificación debe verificar si los cambios hechos al sistema son los que el propietario pidió.

Es importante destacar que los activos sensibles del sistema no deben ser accesados públicamente y que no debe haber usuarios permanentes de este tipo de activos. Cuando se necesite tener acceso a los activos sensibles, se debe de justificar plenamente la necesidad de acceso. Todas las actividades de uso y acceso realizadas por los usuarios, tendrán que ser registradas y revisadas. Los accesos temporales tendrán que ser eliminados inmediatamente después de que se termine la tarea para la cual fue necesario el acceso a los activos sensibles del sistema.

3.4.3 Protección en el Desarrollo

La protección de los activos de información generados o utilizados por una aplicación, debe comenzar a planificarse durante el análisis y diseño o modificación del sistema y consolidarse durante las pruebas que se hacen antes de ponerlo en marcha.

Estos requerimientos son aplicables tanto a los desarrollos hechos dentro de la misma empresa como a los que se encargan a terceras personas y deben permanecer vigentes en las modificaciones posteriores a la aplicación.

Durante el desarrollo, modificación o mantenimiento del sistema o aplicaciones para el mismo, deben crearse datos de prueba para verificar todas y cada una de las opciones de la aplicación, nunca deben de usarse datos reales en las pruebas que se hacen al sistema, ya que su utilización puede comprometer la confidencialidad, integridad y disponibilidad de los activos de la empresa.

Los datos de prueba se pueden guardar después de verificadas todas las opciones del sistema, para ser utilizados cada que se modifique la aplicación.

Separación de los Sistemas de desarrollo y producción. Las actividades de desarrollo y prueba de la aplicación, pueden causar cambios no deseados en los activos de información de producción si comparten el mismo sistema o el mismo entorno operativo. Para evitar este problema, o al menos minimizarlo, deberán de separarse en la medida de lo posible los sistemas en desarrollo de los que ya están funcionando.

3.4.4 Protección de estaciones de trabajo

Los usuarios son responsables de proteger la estación de trabajo que les ha sido asignado, y colaborar en la protección de cualquier otra estación de trabajo de la empresa, para evitar que sea robada o dañada,

que se use la información que contiene esta o que se utilice el sistema al que está conectada esta estación de trabajo.

Cuando se tenga que dejar desatendida la estación de trabajo por más de media hora durante la jornada laboral o cuando finalice ésta, se debe bloquear la terminal utilizando herramientas de bloqueo y arranque por medio de contraseña o si tiene cerradura física utilizarla y guardar la llave en un lugar seguro. Al finalizar la jornada laboral si la estación de trabajo es portátil, es recomendable llevarla consigo o guardarla bajo llave.

Durante los viajes, si se lleva consigo una estación de trabajo portátil es necesario el uso de mecanismos físicos y lógicos de bloqueo y evitar perderla de vista llevándola siempre consigo.

Revisión Periódica. El personal asignado, tendrá que revisar todas las estaciones de trabajo periódicamente (tomando en cuenta que tan confidencial es la información que contiene esa estación de trabajo y que concesiones tiene el usuario de dicha estación de trabajo en los sistemas de información de la empresa; a mayor confidencialidad mas corto el tiempo entre una revisión y la otra) para asegurarse que están debidamente protegidas y que atravez de ellas no se pueda accesar a la información guardada localmente ni a los activos de información contenidos en el sistema o servidor de una red de área local (LAN) al que pueda conectarse.

3.4.5 Cifrado o Criptografía

Criptografía o cifrado es el arte o ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura de tal suerte que solo puedan ser leídos por las entidades a las que van dirigidos.

Las técnicas de encriptación de datos, es transformar la información por medio de algoritmos, de tal manera que no tenga nada que ver con lo que en realidad es, esto con el fin de asegurar, que mientras está viajando, no pueda ser interpretada por personas no autorizadas. Al llegar a su destino, a ésta información, se le aplica otro algoritmo, para devolverla a su estado original.[13]

Las dos técnicas mas sencillas de cifrado, el la criptografía clásica, son la sustitución (que supone el cambio de significado de los elementos básicos del mensaje) y la trasposición (que supone una reordenación de los mismos); la gran mayoría de las cifras clásicas son combinaciones de estas dos operaciones básica.

El descifrado es el proceso inverso que recupera el texto plano a partir del texto cifrado y la clave. [14]

Existen dos formas comunes de encriptar los datos: Llave asimétrica y llave simétrica, la que se utilice depende de las necesidades de cada sistema en particular.

- Llave asimétrica. En el sistema criptográfico de llave pública. Una llave pública es usada para encriptar los datos y una llave secreta es utilizada para des encriptar los datos.

[13] http://es.wikipedia.org/wiki/Criptograf%C3%ADa
[14] http://es.wikipedia.org/wiki/Criptograf%C3%ADa

- Llave simétrica. El mismo algoritmo que sirve para encriptar los datos sirve para desencriptar estos.

Cuando el acceso físico o lógico a los activos de información no pueda ser controlado o por su especial sensibilidad o confidencialidad, requieran medidas adicionales de seguridad, la información tiene que cifrarse de forma que quede ilegible y no pueda ser procesado por ningún usuario o persona no autorizada.

Un activo de información cifrado, para su almacenamiento o envío, mantiene el mismo nivel de clasificación y tiene que ser protegido como el activo original.

Claves de cifrado. Las claves de cifrado y descifrado son una serie de caracteres usados para codificar la información y sin las cuales no serán legible ni podrán ser procesada.

Protección de las claves de cifrado. Para proteger las claves de cifrado se deben definir e implantar los siguientes controles:

- El uso de las claves debe estar restringido a personas autorizadas a realizar las funciones de cifrado.

- El uso de las claves de cifrado debe de ser aprobada por el propietario de la información. El propietario debe de conocer y aprobar que se va a cifrar y que se va a descifrar.

- El propietario de la información puede asignar a una persona o personas de su confianza para delegar formalmente la responsabilidad del servicio de cifrado, así como la aprobación de la utilización de este.

- La clave de cifrado tiene que ser transmitida por un conducto diferente al del activo cifrado.

- Cuando el cifrado y descifrado no se realice por medio de programas, los recursos informáticos tienen que estar protegidos en un área de Acceso Restringido (AAR).

3.4.6 Códigos Maliciosos

Los códigos maliciosos son programas o pedazos de código que corren en la computadora sin darse cuenta y su función es muy diversa, pero básicamente todos tienen la capacidad de reproducirse y una estrategia de propagación.

Los tipos de **Códigos maliciosos** son:

- Virus. Son piezas de código que se instalan en la computadora; los virus son hechos para crear destrucción, su trabajo consiste en borrar archivos del disco duro y hacer muchas copias de ellos mismos, hasta que los recursos de la computadora se agotan.

- Caballo de Troya. Programas que tras una aparente función, encierran en su interior otra función. Pero son muy peligrosos ya que están diseñados para una función en específico, y pueden crear las llamadas puertas traseras para poder violar la seguridad en el sistema.
- Gusano. Está diseñado para buscar zonas de memoria desocupadas donde autocopiarse repetidas veces, hasta que consigue desbordar la memoria del equipo físico. Se puede decir que el gusano tiene la misma función que el virus con la diferencia de que el gusano se reproduce en las redes y el virus solo en un equipo físico especifico.
- Bombas Lógicas. Es un tipo de virus o caballo de troya que solo actúa cuando se da una condición especifica. Por ejemplo una determinada fecha, una secuencia de teclas, etc.

El más extendido es el Virus Informático que suele contener varias de las características descritas.

Para referir a cualquier código malicioso a partir de ahora se utilizará la palabra virus.

Existen, en el mercado, programas Antivirus que detectan la presencia de virus y pueden eliminarlos. Estos programas van siendo actualizados de forma periódica, incorporando protección contra nuevos virus aparecidos. No obstante, siempre se estará expuesto a los virus que no hayan sido incluidos en los programas antivirus, pero el riesgo será mucho mayor si no utilizamos ningún método de prevención y/o eliminación.

Protección en LAN y PC. El arranque del sistema desde un disco removible contaminado o la ejecución de un programa contaminado produce la infección por virus.

Los virus se pueden dividir en dos grandes grupos:

- Virus de programa: Estos virus infectan a ficheros ejecutables (extensiones EXE, COM, SYS, OVL, OVR, etc.)

- Virus de sector de arranque: Estos virus contaminan el sector de arranque de los discos tanto fijos como removibles.

Para eliminar, o al menos minimizar, la infección por virus deben seguirse las siguientes normas:

- Prohibir el uso de productos sin licencia, no autorizados por la empresa o adquiridos de fuentes sin garantía.

- Verificar todo disco removible o fichero recibido que provenga de otro usuario con programas antivirus.

- Tener siempre un antivirus residente en el sistema y actualizar el antivirus utilizado cada que surja una nueva versión.

- Realizar copias de respaldo periódicamente.

- Proteger contra escritura todos los discos removibles.

Cualquier infección que se detecte, tiene que ser notificada al personal a cargo, para el aislamiento de los sistemas afectados, el análisis del virus y su eliminación. También, debe haber una protección para la conexión de los sistemas a una red de área local (LAN), que evite la inclusión de programas no autorizados en las estaciones de trabajo de los usuarios de la red o en los servidores.

Es importante destacar que esta prohibida la propagación conciente de programas o datos infectados con virus ya sea dentro de la empresa o desde ella.

La utilización de un antivirus y la protección de las estaciones de trabajo es responsabilidad del usuario final, pero el departamento de sistemas debe asesorarle para la utilizaron y actualización de programas antivirus.

Protección en Sistemas Corporativos. Ya que la conexión de los sistemas y las redes a otros sistemas y redes significa un importante riesgo de seguridad tanto para la red en si como para los sistemas conectados a ella y para la información que contiene los sistemas, debe tenerse un control de todas las transferencias de activos recibidas, asegurándose que ningún activo es o contiene algún virus informático. Se debe de poner un cuidado especial en los programas ejecutables recibidos.

Esto se logra, instalando filtros en los puntos de entrada de la red y los sistemas, cuya función es aislar y suprimir los activos o códigos dañinos.

Estos filtros pueden ser cortafuegos, ruteadores, switches, entre otros.

- **Cortafuegos(Firewall).** Un cortafuego es un componente puesto entre la computadora y la red para ayudar a eliminar accesos indeseados provenientes del exterior. Puede estar compuesto por software, hardware o una combinación de las dos.

  Un cortafuegos es por lo general un modo de construir un muro entre una parte de una red (por ejemplo la red interna de una organización) y otra parte (por ejemplo Internet), con la particularidad de que es necesario permitir que algún tipo de tráfico, con unas características determinadas, pase a través de ciertas puertas cuidadosamente vigiladas.

  La parte difícil está en establecer los criterios por los que se permite o deniega el paso a través de las puertas.

- **Ruteadores.** Una de las mejores características de seguridad de los ruteadores es la habilidad de filtrar paquetes, ya sea por dirección de origen, dirección destino, protocolo o puerto.

- **Switches.** Ya que los switches son configurables, implementando una seguridad adecuada con los switches se puede configurar de tal forma que la seguridad que proporcione sea similar a la que proporciona un firewall o un ruteador.

- **VPN.** Las VPN son redes privadas virtuales que forman un túnel que comunique a las redes locales de la empresa en las diferentes localizaciones geográficas. De esta forma se puede tener acceso remoto a las redes locales de la empresa de una manera segura ya que se utilizan mecanismos de encriptación

3.5 Gestión de la autoridad del sistema

La autoridad del sistema es la concedida a un usuario por asignación de atributos, privilegios o derechos de acceso que están asociados con la operatividad del sistema y que son necesarios para realizar actividades de soporte, mantenimiento y operación del propio sistema.

Debe sancionarse a los usuarios que usen este tipo de autoridad de manera inapropiada para obtener algún beneficio. Esta situación es considerada como abuso de autoridad.

Los derechos de acceso a la información del sistema deben de cumplir las siguientes normas:

1. Los accesos a los activos de información del sistema, que no sean accesibles por un usuario general, tienen que estar basados en una necesidad de acceso válida y vigente, aprobada por el departamento de sistemas de información. Los usuarios cuyas responsabilidades incluyan el mantenimiento y soporte del sistema, están exentos de tener autorización escrita para acceder a ellos.

2. Los identificadores de usuario definidos para automatizar la operatividad pueden ser considerados como parte integrante del sistema y asignados a un departamento de soporte y mantenimiento de sistemas, en vez de a un individuo. Los usuarios que puedan manejar este tipo de identificadores deben tener una necesidad de uso por razones de negocio válida y vigente, aprobada por el departamento de sistemas de información.

3. Los accesos a los activos de información del sistema pueden ser implantados concediendo el acceso a un grupo de usuarios, siempre que cada acceso de un miembro del grupo pueda ser identificado individualmente. El departamento de sistemas de información debe tener definido e implantado un proceso, incluyendo revisiones periódicas, que asegure la permanente actualización de la lista de acceso y la eliminación de accesos cuando ya no sean necesarios.

4. Las actividades realizadas con autoridad de sistema tienen que estar específicamente autorizadas por la Dirección, por un proceso de control de cambios, o tienen que ser consistentes con la descripción del puesto de trabajo del usuario que la realiza. El departamento de sistemas de información tiene que asegurarse que los usuarios que tienen esta autoridad, están informados de ello.

3.6 Gestión de la autoridad de administración de seguridad

El objetivo de la gestión de la autoridad de administración de seguridad es asegurarse que sólo los usuarios autorizados pueden añadir, modificar o eliminar funciones de administración de seguridad del sistema.

La autoridad de administración de seguridad es la concedida a un usuario por asignación de atributos o privilegios que están asociados con el sistema de control de acceso y que son necesarios para realizar las actividades de control y administración de seguridad del propio sistema.

Debe sancionarse a los usuarios que usen este tipo de autoridad de manera inapropiada para obtener algún beneficio. Esta situación es considerada como abuso de autoridad.

Para asignar la autoridad de administración de seguridad se deben de cumplir los siguientes puntos:

1. Generalmente, La autoridad de administración de seguridad es asignada a un solo usuario, pero también puede ser asignada a un grupo de usuarios o a un usuario automático.

   La asignación de este tipo de autoridad debe de cumplir las condiciones siguientes:

   - La identificación de cada uno de los miembros del grupo debe ser individual.

   - Todos y cada uno de los usuarios con este tipo de autoridad deben de cumplir todas las reglas de este apartado, como si ellos fueran usuarios únicos con este tipo de autoridad.

2. La asignación de este tipo de autoridad a un usuario por mas de un mes, debe ser aprobada por escrito por el departamento de sistemas de información y revalidada cada año.

3. La asignación de este tipo de autoridad a un usuario por hasta un mes, debe ser aprobada primero por el departamento de sistemas de información, aunque si es una emergencia se puede dar primero la concesión de autoridad y después la aprobación.

4. Las actividades realizadas con autoridad de administración de seguridad tienen que estar específicamente autorizadas por la dirección, por un proceso de control de cambios, o tienen que ser consistentes con la descripción del puesto de trabajo del usuario que la realiza. La función del departamento de sistemas de información es asegurarse que los usuarios, que tienen esta autoridad, están informados de ello.

5. Todas las actividades realizadas con este tipo de autoridad tienen que ser registradas, siempre y cuando el sistema de control de accesos lo permita. El registro de estas actividades nunca debe ser desactivado.

   Para el registro de estas actividades se tiene que definir:

   - El formato y el contenido de los documentos para la aprobación por escrito de la autoridad de administración de seguridad.

   - Un procedimiento para la asignación y aprobación de esta autoridad a corto plazo y en emergencia.

   - Un procedimiento para la cancelación de esta autoridad cuando la necesidad de un usuario finaliza.
   - Un procedimiento para detectar y corregir cualquier asignación de esta autoridad adquirida sin autorización, incluyendo el bloqueo del usuario que la ha obtenido.

3.7 Registros de intentos de acceso

La creación de este tipo de registros podrá llevarse a cabo si existe un apropiado sistema de control de accesos. Estos registros deberán guardarse al menos durante un año.

Servirán de base para el análisis de cualquier incidente de seguridad relacionado con los sistemas de información y como documentos a revisar en cualquier auditoria.

3.7.1 Registros de Acceso al Sistema

Tienen que ser registrados los accesos al sistema y los intentos de acceso inválidos.

Es importante tener estos registros, ya que el personal encargado de evaluar e instalar la seguridad en el sistema, podrá darse cuenta la cantidad de usuarios que tienen acceso al sistema así como también la cantidad de intentos de acceso por usuarios no autorizados; con esta información se podrá decidir más claramente si la seguridad del sistema es la adecuada o si necesita reforzarse. Cabe mencionar que se está hablando del acceso al sistema, no a la información del sistema que son los activos de información.

3.7.2 Registros de Acceso a Activos

Tienen que ser registrados los accesos a activos de información y los intentos de acceso inválidos.

La utilización de estos registros, es importante, ya que ayudará al personal encargado de evaluar e instalar la seguridad en los activos del sistema a conocer la cantidad de usuarios que tienen acceso a estos activos, así como también la cantidad de intentos de acceso por usuarios no autorizados; con esta información se podrá decidir más claramente si la seguridad sobre los activos es la adecuada o si necesita reforzarse.

3.7.3 Registros de Actividades

Las actividades realizadas usando la autoridad de sistema y la autoridad de administración de seguridad tienen que ser registradas y su registro nunca puede ser desactivado.

Es importante tener estos registros, ya que el personal autorizado para la evaluación e implantación de seguridad en el sistema, podrá darse cuenta si existen usuarios no autorizados intentando manipular o manipulando los activos sensibles del sistema o la seguridad del mismo. También estos registros permitirán conocer si el personal autorizado para la manipulación de datos sensibles y la seguridad está actuando correctamente.

3.8 Informes de violación de acceso

El objetivo de los informes de violación de acceso es asegurarse que los intentos de acceso no autorizado al sistema o a los Activos del sistema, pueden ser reconocidos como una violación, inmediatamente o después del consiguiente análisis.

El uso de estos informes es importante, ya que con ellos los responsables de la seguridad del sistema y los dueños de la empresa, tendrán conocimiento del interés por parte de atacantes por la información del sistema y podrán planear una mejor estrategia de seguridad para evitar la violación del sistema.

3.8.1 Accesos Inválidos al Sistema

Deben de estar definidos controles que limiten las veces que un usuario puede intentar tener acceso al sistema. Estos controles deben de incluir el bloqueo del identificador de usuario a partir de determinados intentos de autenticación.

El departamento de sistemas de información debe tener definido e implantado un proceso que le permita obtener informes de los intentos fallidos de acceso al sistema, cuando sean solicitados.

Ataques Sistemáticos. El departamento de Sistemas de Información deberá tener definido e implantado un proceso o controles que le permita detectar, gestionar e informar cuando se produzca un excesivo número de intentos de acceso inválidos al sistema o bloqueo sistemático de usuarios. Para evitar estimaciones subjetivas, cada sistema debe tener previamente fijado un límite a partir del cual se considera que está siendo atacado de forma sistemática. Estos informes permiten, al personal autorizado, la planeación e implantación de una seguridad reforzada en las áreas mas atacadas.

2.8.2 Accesos Inválidos a Activos

El departamento de sistemas de información debe tener definido e implantado un proceso que le permita obtener informes de los intentos fallidos de acceso a activos, cuando sean solicitados.

Estos informes permiten, al personal autorizado, la planeación e implantación de una seguridad reforzada en las áreas mas atacadas.

CAPÍTULO CUARTO: *Políticas y diagnósticos de seguridad*

En este capítulo se dejará clara la importancia de tener una buena política de seguridad, ya que ésta permitirá manejar el sistema de una manera más segura. Las políticas de seguridad son normas de seguridad que sigue toda la empresa.

Otro tema importante que se tratará en este capitulo es el diagnóstico de la seguridad, es decir evaluar el sistema en cuanto a su seguridad y así poder corregir lo que no esté funcionando correctamente.

4.1 Políticas de seguridad

Como ya se ha dicho con anterioridad, es de suma importancia la seguridad en los sistemas de información ya que ésta, representa activos valiosos para las empresas u organizaciones, es decir, se necesita tener suficiente confianza o seguridad de que la información o datos que arrojen los sistemas sean verídicos.

Desgraciadamente en nuestros días, toda la información de cualquier empresa es atractiva para personas que desean manipularla de forma incorrecta, o que desean obtener beneficios de ésta, por lo que se vuelve cada día más importante tener un buen sistema de seguridad que nos permita proteger la información para que no pueda ser violada tan fácilmente.

El objetivo principal de la seguridad en los sistemas de información, es asegurar que el sistema arroje datos correctos y cifras exactas del estado de la empresa u organización.

Implantar un buen sistema de seguridad en los sistemas de información, es siempre rentable a largo palazo, ya que se evitarán muchos problemas que se tendrían con un sistema sin seguridad.

Al desarrollar un sistema se debe de implantar la seguridad como otra parte del sistema, ya que un sistema de seguridad, es sinónimo de muchos costos a largo plazo y muchos errores.

Las decisiones de seguridad que se lleven a cabo en un sistema de información, así como las que no se tomen en cuenta, determinarán lo seguro o no seguro que será el sistema, por lo tanto no pueden tomarse decisiones acertadas en materia de seguridad, si no se conocen los objetivos claramente.

Los **objetivos** se determinarán de acuerdo a lo siguiente:[15]

- **Servicios ofrecidos frente a la seguridad proporcionada:** Cada servicio ofrecido a los usuarios lleva consigo sus propios riesgos de seguridad.

- **Facilidad de uso frente a seguridad:** El sistema más fácil de usar permitiría el acceso a cualquier usuario y no requeriría la autentificación mediante ningún método. El uso de métodos de autenticación, hace el sistema mas seguro aunque también más incomodo.

- **Costo de la seguridad frente al riesgo de pérdida:** Hay muchos costos que conlleva la seguridad como son los monetarios (por ejemplo, el gasto en adquirir hardware y software de seguridad, como podrían ser un cortafuegos –en caso de que sea un sistema utilizado a través de la red- o generadores de contraseñas de un solo uso), en rendimiento (el cifrado y descifrado llevan tiempo), y en facilidad de uso como ya se ha mencionado. En toda situación cada tipo de costo orientado a mejorar la seguridad de un sistema debe ser sopesado frente al tipo de pérdida que supondría no establecerlo.

- **Costo de la no-seguridad:** Fundamentalmente, éstos son debidos a daños producidos por la no puesta en práctica de acciones preventivas que sirvan para prevenir los riesgos a los que se ven sometidos los sistemas de información como son la pérdida de

[15] http://www.csi.map.es/csi/silice/Segurd6.html

privacidad (por ejemplo, la lectura de información por personas no autorizadas), pérdida de datos (eliminación o corrupción de la información), y la degradación del servicio (por ejemplo, la saturación del espacio de almacenamiento y el abuso de recursos).

Los objetivos de seguridad de la empresa deben de ser comunicados a todos los miembros que laboren en dicha empresa.

En base a los objetivos de la empresa, se determinarán las **políticas de seguridad.**

Políticas de seguridad

Las políticas de seguridad, son una serie de normas que se seguirán en la empresa con el fin de garantizar la seguridad en el acceso a los sistemas de información, como podría ser el uso de contraseñas distintas dependiendo la persona o el puesto que tenga dicha persona en la empresa.

El principal objetivo de las políticas de seguridad, es informar a todos los miembros de la empresa, sobre los requisitos que se tendrán en el sistema de información, con el fin de asegurar el buen uso del sistema.

Para que las políticas de seguridad en una empresa funcionen correctamente, es muy importante contar con el apoyo de todos los niveles de la organización, con el fin de trabajar conjuntamente hacia una meta común, de lo contrario seria muy poco probable que esta política tuviera el éxito deseado.

Para lograr que estas políticas sean aceptadas y la seguridad adecuada dentro de la organización, se deben de involucrar a la mayoría

de las personas de dicha empresa, empezando desde los técnicos que meten la información, hasta los altos directivos.

Con el tiempo, las políticas de seguridad de las empresas, sobre todo las que están en desarrollo se irán adecuando a las necesidades actuales de dicha organización, es por esto que se dice que las políticas de seguridad deben de ser flexibles.

Una buena política de seguridad debe incluir los siguientes componentes: [16]

- **Guías para la Adquisición de Tecnología de la Información:** Especificación de las características de seguridad requeridas o deseadas. Deben ser un suplemento a otras guías para la adquisición de bienes y servicios.

- **Política de Privacidad:** Definición de la privacidad que se desea en cuanto a control del correo electrónico, o el acceso a los ficheros de los usuarios en caso de que sea un sistema de red.

- **Política de Acceso:** Definir los derechos de acceso con el fin de proteger los activos de la pérdida o alteración, especificando las pautas de uso responsable para los usuarios, el personal técnico y los directivos. Debe proporcionar normas precisas en lo que se refiere a conexiones externas, transmisión de datos, conexión de dispositivos a una red, e instalación de nuevo software en los diferentes sistemas.

[16] http://www.csi.map.es/csi/silice/Segurd9.html

- **Política de Registro:** Especificar de qué tipo de acciones se lleva una contabilidad pormenorizada, procedimientos de auditoria y la forma de actuar en caso de que a partir de esta se detecte un incidente.

- **Política de Autenticación:** Establecer políticas efectivas de contraseñas y definir los mecanismos para la autenticación remota y el uso de dispositivos de autenticación.

- **Declaración de Disponibilidad:** Establecer las expectativas de los usuarios en relación a la disponibilidad de los recursos. Se debe especificar el horario en que se garantiza la operatividad de los sistemas y los períodos de indisponibilidad por mantenimiento. Se debe asimismo señalar el procedimiento para informar de fallos en los sistemas y la red.

- **Política de Mantenimiento:** Describir en qué términos se autoriza al personal de mantenimiento, tanto interno como externo, para acceder a los sistemas y manejar éstos. Un punto importante es si se permite o no el mantenimiento remoto y, en su caso, cómo se controla.

- **Política de Notificación de Incidentes:** Indicar qué tipo de violaciones a la política de seguridad deben notificarse y a quién se debe hacer.

- **Información de Soporte:** Indicar a los usuarios, personal de los distintos departamentos y directivos, a quién deben dirigirse cuando detecten algún problema relativo a la seguridad.

4.2 Diagnóstico de la seguridad

Deben de planificarse actividades anualmente para verificar el sistema de seguridad implantado, esto incluye verificar si el nivel de implantación es el correcto o si existen carencias o deficiencias. Por ejemplo si permite la intrusión de personas no autorizadas, o esté contaminado de algún virus, etc.

Las actividades a realizar por el equipo encargado de hacer el diagnóstico de la seguridad en el sistema de información pueden dividirse en: Autoevaluación, Revisión, Auditoria.

- **Autoevaluación.** Es cuando la revisión del sistema de seguridad está a cargo de un equipo que pertenece a la misma función que se está evaluando.

- **Revisión.** En esta actividad se debe de verificar que se estén cumpliendo todas las normas y procedimientos establecidos en la política de seguridad de la empresa, y observar todas las deficiencias.

  Las desviaciones y deficiencias detectadas se capturarán en un informe que se entregará a la dirección. Este informe aparte debe de contener las recomendaciones para la corrección de estas deficiencias.

- **Auditoria.** Es cuando la revisión está a cargo de un departamento auditor, ya sea de la empresa o exterior. Y se define igual que la revisión.

  Dependiendo del alcance una auditoria puede ser:

  - Funcional. Cuando solo afecta a una parte de la empresa.
  - Total. Cuando afecta a toda la empresa, incluyendo la función de sistemas de información.

Los requerimientos mínimos para un buen diagnósticos son:

- **Una autoevaluación por función cada año**.

- **Revisión funcional por función cada año.**

- **Una revisión funcional en el sistema de información que debe de ser cada año**.

- **Una revisión total del sistema de la empresa cada tres años.**

- **Una auditoria total del sistema de la empresa cada tres años.**

Al realizar estas pruebas, podremos asegurar resultados satisfactorios. Un resultado insatisfactorio en cualquiera de estas pruebas obliga su repetición antes de seis meses de haberla hecho.

La revisión o auditoria total del sistema de la empresa y la revisión funcional de sistemas de información tienen que incluir pruebas de

integridad de sistemas (Probar si nadie puede tener acceso al sistema de manera ilegítima por ejemplo).

La valoración individual de cada uno de los hechos que se producen durante una revisión o auditoria es muy importante.

La siguiente tabla de la Fig. 4.1 es un formato de como hacer la evaluación de la seguridad en la auditoria o revisión tomando en cuenta la clasificación de la información y la existencia o no existencia de una norma de seguridad en la implantación.

Fig.4.1 Formato de Evaluación se Seguridad

Información Afectada	Norma Implantada	Norma Parcialmente Implantada	Norma No implantada
Pública			
Interna			
Confidencial			
Secreta			

Al término de cada revisión o auditoria debe crearse un informe de resultados que será presentado al más alto nivel de dirección afectado y una copia enviada al director de seguridad.

Las desviaciones o deficiencias detectadas deben generar un plan de acción, encaminado a su corrección, incluyendo responsable de la actividad y fecha de terminación.

Este plan tiene que ser realizado antes de 30 días, cuando por ejemplo se encontraron deficiencias en la seguridad de la información confidencial, es decir cuando la no seguridad puede afectar gravemente la integridad de la información del sistema, si no es tan riesgosa la no seguridad, se puede tomar un poco más de tiempo para corregir el problema.

CAPÍTULO QUINTO: *Ejemplo práctico: Sistema de inventario para la tienda de ropa y accesorios para bebe "Periquita"*

En éste capítulo se realizará un sistema de inventario para la tienda de ropa y accesorios para bebé "Periquita"; se analizarán los problemas actuales de este negocio en cuanto a seguridad en el acceso a la información, y se realizarán los cambios adecuados para tener un sistema de información seguro y adecuado para la empresa en cuestión.

CAPÍTULO QUINTO: *Ejemplo práctico: Sistema de inventario para la tienda de ropa y accesorios para bebe "Periquita"*

5.1 Descripción y Forma de Operar del Negocio

Es importante conocer todas las actividades que realiza el negocio en cuestión, para poder incluirlas todas en el sistema que se realizará. En los siguientes puntos se explicará todo lo referente al negocio:

❖ Descripción del Negocio

- **Nombre del Negocio:** Tienda de Ropa y Accesorios "Periquita"
- Giro: Venta de Ropa y accesorios para bebé de 0 a 5 años de edad.
- **Cantidad de personas laborando en el Negocio**: 3 personas; de las cuales, 2 son empleados y 1 es el dueño del negocio.

❖ Forma de operar del Negocio

- **Al hacer una venta:** Cuando el negocio hace una venta, entrega al cliente una nota de remisión con los datos de los artículos que compró, el importe total de la compra y los datos del negocio (Nombre, dirección, teléfono, RFC, Correo electrónico).
- **Al comprar Mercancía:** Cuando la tienda de ropa hace una compra de mercancía a proveedores, estos le entregan al negocio notas de remisión o facturas de los productos adquiridos.
- **Al hacer el inventario:** El inventario lo hacen los empleados junto con el dueño, cuentan artículo por artículo y lo anotan

en unas hojas que contienen los siguientes datos: nombre del artículo, nombre del proveedor o proveedores, cantidad de artículos, precio por unidad y fecha de elaboración del inventario. Ya que este procedimiento es muy tedioso y tardado, no se realiza con la frecuencia deseable, además de que puede tener los clásicos "Errores de dedo".

5.2 Riesgos de Seguridad

En esta sección, se analizaran, definirán y ubicarán todos los riesgos de seguridad que tiene este negocio (en cuanto a salvaguarda de la información) con la forma actual de operar del mismo, para este fin, se tomarán como base los puntos explicados en el capitulo uno, sección uno punto tres de esta tesis.

- **Activos**: Notas de remisión de ventas; notas de remisión o facturas de compras a proveedores; inventarios.

- **Amenazas:** Incendios, robo de información, manipulación de información.

- **Vulnerabilidades:** Ya que toda la información está en papel, y guardada en un cajón del mismo negocio, es muy fácil que personas

no autorizadas tengan acceso a ella y la manipulen, quemen, rompan o extravíen.

- **Impacto:**
  - **Impacto cuantitativo:** Se puede robar mercancía y dinero, alterando o extraviando las notas de remisión de ventas, las notas de remisión y facturas de compras y/o los inventarios.
  - **Impacto cualitativo con pérdidas orgánicas:** Se puede despedir o efectuar acción penal sobre alguna persona inocente, inculpándola injustamente.
  - **Impacto cualitativo con pérdidas funcionales:** Con la pérdida de información, la tienda no estará funcionando correctamente ya que no se tendrá ningún control del mismo.

- **Riesgos:** Pérdidas en dinero para el negocio; información errónea en los inventarios, notas de remisión de ventas y notas de remisión o facturas de compras.

- **Defensas:** Toda la información del negocio, se guardan en un cajón de la oficina del negocio.

Como se observa, los riesgos de seguridad en este negocio son muchos actualmente, ya que la información no está debidamente organizada ni protegida. Por este motivo es importante que se realice un

sistema de información para este negocio incluido un adecuado sistema de seguridad.

5.3 Desarrollo de un sistema de inventario para este negocio

Se realizará un sistema de información apropiado para este negocio, que residirá en un solo equipo de cómputo y que controlara:

- **Existencias:** Tener un control exacto de todos los artículos. Tipo de artículos que tiene la tienda, cantidad de artículos de cada tipo, datos de proveedores, etc. Básicamente todo lo que tenga que ver con los artículos que vende esta tienda.

- **Ventas:** Controlar todas las ventas que hace la tienda.

- **Mecanismo de seguridad en el acceso al sistema de información:** Utilización de un buen método de seguridad que evitará que personas no autorizadas consulten y/o modifiquen la información del sistema de inventario.

5.3.1 Planeación del sistema de inventario para la tienda de ropa y accesorios para bebe "Periquita"

Con la planeación del sistema se explicarán todos los requerimientos de salida que tiene el sistema, es decir cómo y el cuándo debe el sistema arrojar los datos procesados.

También se especificará toda la información que necesita el sistema para poder cumplir con los requerimientos de salida que tiene el sistema. Y por último los requerimientos de equipo que tendrá este sistema.

- **Requerimientos**

  - **Requerimientos de salida:** Todos los resultados que debe de arrojar el sistema.

    - *Reporte de inventario.* Se requiere que el sistema elabore reportes de inventario con los siguientes datos: nombre del negocio, dirección del negocio, teléfono del negocio, fecha de elaboración del reporte, clave clasificación del artículo(Los artículos estarán clasificados por tipo de artículo: Blusas, camisas, pantalones, pantalones cortos, faldas, vestidos, conjuntos, ropa interior, aretes, cinturones, adornos para la cabeza), clave del artículo, Nombre del artículo, precio de compra, precio de venta, máximo de artículos permitidos en bodega, mínimo de artículos permitidos en bodega, clave de proveedores, organizado todo por clave y nombre de clasificación del

artículo. Estos reportes se tendrán que elaborar semanalmente o cuando el usuario lo desee.

- *Reporte de nombres de clasificaciones de artículos.* Es deseable que el sistema elabore este tipo de reporte, para que el usuario pueda consultarlo cuando lo requiera con los siguientes datos: nombre del negocio, dirección del negocio, teléfono del negocio, fecha de elaboración del reporte, clave clasificación del artículo, nombre clasificación de artículo, clave de artículo, nombre de artículo. Organizado este reporte por nombre de la clasificación del artículo.

- *Reporte de proveedores.* Se requiere, que el sistema elabore reportes de proveedores con los siguientes datos: nombre del negocio, dirección del negocio, teléfono del negocio, fecha de elaboración del reporte, clave de proveedor, nombre de proveedor o de la empresa proveedora, dirección, teléfono, RFC, clave de la clasificación del artículo que vende, nombre del artículo o artículos que vende, el reporte se elaborará cada que el usuario lo pida. Estos reportes estarán organizados por nombre del proveedor.

- *Reportes de ventas diarias.* Se elaborarán reportes diarios de todas las ventas del día con los siguientes

datos: nombre del negocio, dirección del negocio, teléfono del negocio, fecha de elaboración del reporte, clave del artículo, nombre del artículo, precio de compra del artículo, precio de venta del artículo, ganancia, y total de ganancias del día. Organizados estos reportes por nombre del artículo.

- *Reportes de ventas.* Con el fin de saber exactamente como está funcionando el negocio, es deseable realizar reportes de ventas semanales, mensuales y anuales, el reporte tendrá que contener los siguientes datos: nombre del negocio, dirección del negocio, teléfono del negocio, fecha de elaboración del reporte, clave del artículo vendido, nombre del artículo vendido, su precio unitario de venta, importe total de todos los artículos vendidos del mismo tipo y el total de todos los artículos vendidos en esa semana, mes o año. Todos organizados día, mes o año.

- *Reporte de ganancias.* Para llevar un control exacto de las ganancias del negocio, es deseable elaborar reportes semanales, mensuales y anuales con los siguientes datos: nombre del negocio, dirección del negocio, teléfono del negocio, fecha de elaboración del reporte, clave del artículo, nombre del artículo, precio unitario de venta del artículo, precio unitario de compra del

artículo, ganancia por unidad, ganancia por tipo de artículo, y ganancias totales en esa semana, mes o año. Organizados estos reportes por días, semanas o meses respectivamente.

- *Reporte de dinero invertido*. Para poder saber exactamente cuanto dinero está invertido en el negocio, es deseable que el sistema elabore reportes que arrojen los siguientes datos: nombre, dirección y teléfono del negocio, fecha de elaboración de reporte, clave de la clasificación del artículo, clave del artículo, nombre del artículo, numero de artículos en existencia del mismo tipo, precio de compra unitario, precio de venta unitario, total en dinero de cada tipo de artículo de compra y de venta, total en dinero de venta y de compra de todos los tipos de artículos. Organizados todos los reportes por tipo de artículo. Estos reportes se elaboraran mensualmente o cada que el usuario lo desee.

- *Reporte de artículos más vendidos*. Es deseable que el sistema elabore reportes a cerca de los artículos más vendidos en un determinado lapso de tiempo con los siguientes datos*:* nombre del negocio, dirección del negocio, teléfono del negocio, fecha de elaboración del reporte, clave del artículo, nombre del artículo, precio de

venta, precio de compra, número de artículos vendidos en ese lapso de tiempo, clave del proveedor, nombre del proveedor. Este reporte se elaborará mensualmente o cada que el usuario lo desee.

- *Reporte de artículos menos vendidos.* Es deseable que el sistema elabore reportes a cerca de los artículos menos vendidos en un determinado lapso de tiempo con los siguientes datos*:* nombre del negocio, dirección del negocio, teléfono del negocio, fecha de elaboración del reporte, clave del artículo, nombre del artículo, precio de venta, precio de compra, número de artículos vendidos en ese lapso de tiempo, clave del proveedor, nombre del proveedor. Este reporte se elaborará mensualmente o cada que el usuario lo desee.

- *Notas de venta.* Es deseable que el sistema elabore notas de venta cada que algún cliente realice una compra, esta nota tendrá que contener los siguientes datos: nombre del negocio, dirección del negocio, teléfono del negocio, correo electrónico del negocio, RFC del negocio, fecha de elaboración del la nota, numero de folio, clave del artículo, nombre del artículo, precio por unidad, cantidad, importe por cada tipo de artículo, importe total de la compra.

- *Nómina.* Para que el dueño pueda saber el rendimiento de cada uno de sus empleados, se requiere que el sistema elabore reportes con las ventas hechas por cada empleado con los siguientes datos: nombre del negocio, dirección del negocio, teléfono del negocio, fecha de elaboración del reporte, clave del empleado, nombre del empleado, número de folio de la venta hecha, importe total de la venta; organizado por nombre del empleado. El reporte se elaborará semanalmente o cada que el usuario lo desee.

- **Requerimientos de Entrada.** Todos los datos que el sistema tiene que recibir para poder operar adecuadamente.

  - *Datos.* El sistema requiere para poder funcionar que se cargue en su base de datos toda la información de productos, proveedores, empleados y negocio

  - *Factura o nota de remisión de compra.* Para poder actualizar el inventario del negocio, es necesaria la factura o la nota de remisión que entrega el proveedor, de la cual se tomar los siguientes datos: nombre del artículo, precio de compra, cantidad de artículos.

    Si el proveedor es nuevo, se tomarán todos los datos del proveedor (Nombre del proveedor, dirección del proveedor, teléfono del proveedor, RFC).

- *Notas de venta.* Para hacer algún reclamo o devolución de un artículo, es necesario que el cliente presente la nota de venta expedida por el negocio, y así poder hacer la modificación en la base de datos.

- **Requerimientos de equipo.** El software necesario para la programación del sistema de información y el hardware requerido para que este sistema funcione apropiadamente.
  - *Programas*. Como este estudio no abarca la programación de este sistema, solo se dirá que se necesita un lenguaje de programación y un manejador de bases de datos.

  - *Memoria Ram:* De 256 a 512 megas en Ram

  - *Capacidad en disco duro*: 20 G como mínimo

  - *Procesador*: Pentium III a 500 Mhtz o su equivalente como mínimo

  - *Unidad para CD*(CDR y CDW)

- *Sistema operativo*. El más utilizado todavía es el Windows, así que se utilizará este sistema operativo en su versión 98 como mínimo. Sin embargo se utilizará el Windows XP porque es el que tiene el equipo de cómputo adquirido por el negocio en cuestión.

5.3.2 Planeación del sistema de seguridad

En este punto se planeará la seguridad lógica y física más apropiada para evitar el acceso no autorizado a éste sistema.

Es importante recordar que entre más grande y/o más privada sea la información que manejará el sistema, más importante y minuciosa será la implantación de barreras físicas y lógicas contra atacantes.

Tomando en cuenta lo anterior, es que se planeará la seguridad física y lógica para este sistema.

5.3.2.1 Objetivo del sistema de seguridad

Evitar que los datos del sistema de información, sean manipulados, borrados o copiados por personas no autorizadas.

5.3.2.2 Seguridad Lógica

Este sistema utilizará métodos de identificación y autenticación de usuario para la seguridad en el software. En los puntos siguientes se explicará paso a paso.

- **Antivirus.** La computadora que contiene el sistema, debe de tener instalado un antivirus que será actualizado cada que sea necesario.

- **Seguridad en el sistema operativo.** Para disminuir el riesgo de que personas no autorizadas tengan acceso al sistema, se especificará una cuenta de usuario con identificador de usuario y autenticación de usuario que en este caso será una contraseña. Digamos que el identificador de usuario sea PERIQUITA, y la contraseña A04BST.

- **Seguridad en el sistema de información.** La seguridad en este sistema, se implantará al inicio del sistema, pidiendo la identificación y autentificación del usuario, y dependiendo el tipo de usuario, se le permitirán o no ejecutar acciones sobre el sistema.

  Identificación de usuario. El sistema tendrá un identificador de usuario para el propietario del negocio, y un identificador de usuario compartido para los empleados.

  Para que el sistema sea más funcional, el sistema incluirá los siguientes métodos:

- *Autorización de nuevo usuario.* Cuando se quiera cambiar el nombre del identificador de usuario del propietario y/o de los empleados, se utilizará este método, siempre y cuando el usuario se identifique como el propietario del negocio.
- *Eliminación de usuario del sistema*. Cuando se quiera eliminar un identificador de usuario, se utilizará este método, que estará disponible solo si el usuario se identifica como el propietario del negocio.

Autenticación de usuario. El método de autenticación de usuario que utilizará este sistema, es por medio de contraseñas.

La contraseña debe ser personal y confidencial; también tendrá la cualidad de que cuando sea tecleada, no se visualizará en la pantalla, sino que cada carácter que sea parte de la contraseña será sustituido por un asterisco.

Para que el sistema sea más funcional, el sistema incluirá el siguiente método:

- *Restauración de contraseñas.* Cuando se desea cambiar la contraseña de un usuario, se utilizará este método, siempre y cuando el usuario se identifique como el propietario del negocio.

CAPÍTULO QUINTO: *Ejemplo práctico: Sistema de inventario para la tienda de ropa y accesorios para bebe "Periquita"*

Concesiones del sistema según el tipo de usuario. Como ya se dijo, existirán dos tipos de usuario, y cada tipo de usuario tendrá concesiones diferentes.

- *Propietario del negocio.* Este tipo de usuario, tendrá acceso total a toda la información del sistema, y podrá manipularla como el desee, excepto a los activos sensibles del sistema (El código del sistema, y la estructura de la base de datos) que son propiedad del programador.

- *Empleados.* Este tipo de usuarios, tendrán acceso más restringido, ya que solo podrá añadir información al sistema (Capturar datos y hacer nuevas ventas).

Seguridad en los activos sensibles del sistema. Los activos sensibles de este sistema son, el código del sistema (La programación) y la estructura de la base de datos.

La integridad del sistema será garantizada, utilizando el método de contraseña de acceso a la base de datos del sistema, cifrando la tabla de autenticación de usuario e instalando solo ejecutable del sistema de información.

Registros de intentos de acceso al sistema. El sistema tendrá un método que cerrará el sistema después de tres intentos fallidos de identificación o autenticación.

5.3.2.3 Seguridad Física

La seguridad física apropiada para este negocio, se explicará en los siguientes puntos:

- **Seguridad en el Control de Acceso.** El control de acceso físico a el equipo de cómputo que contiene el sistema estará determinado como sigue:
  - No permitir que personas no autorizadas, tengan acceso al equipo de cómputo que contiene el sistema.
  - Cuando la jornada laboral termine y el negocio se quede solo, es importante cerrar todas las posibles áreas de acceso al equipo de cómputo.
  - No dar información de acceso al sistema a personas ajenas al negocio.

- **Ambiente.** Para cuidar el ambiente donde residirá el equipo de cómputo, se deberán de cumplir los siguientes puntos:
  - *Protección de datos.* Para evitar que la información del negocio se pierda en caso de que el equipo de cómputo resulte dañado, se realizarán copias de seguridad cada mes de todos los datos del sistema llamadas respaldos completos.

    Cada copia se hará en un disco compacto.

También se tendrá una copia del sistema, para prevenir la pérdida del sistema.

Estas copias serán resguardadas por el dueño del negocio, preferentemente en un lugar totalmente cerrado y con protección contra incendios (Caja Fuerte).

5.3.3 Estructura de la base de datos

Para la elaboración de la base de datos y las pantallas del sistema, este estudio utilizó Microsoft Access 2000 y Visual Basic 6 respectivamente.

La base de datos que almacenará la información del negocio está constituida por las siguientes tablas, cada una de las cuales contiene información relacionada con su nombre.

- ClasificacionProd
- Empleado
- Producto
- Venta
- Propietario
- Ventaproducto
- Productoproveedor
- Negocio

- Proveedor
- Identificacionusuario
- Autentificaciónusuario

Fig. 5.1 Campos que contiene cada tabla

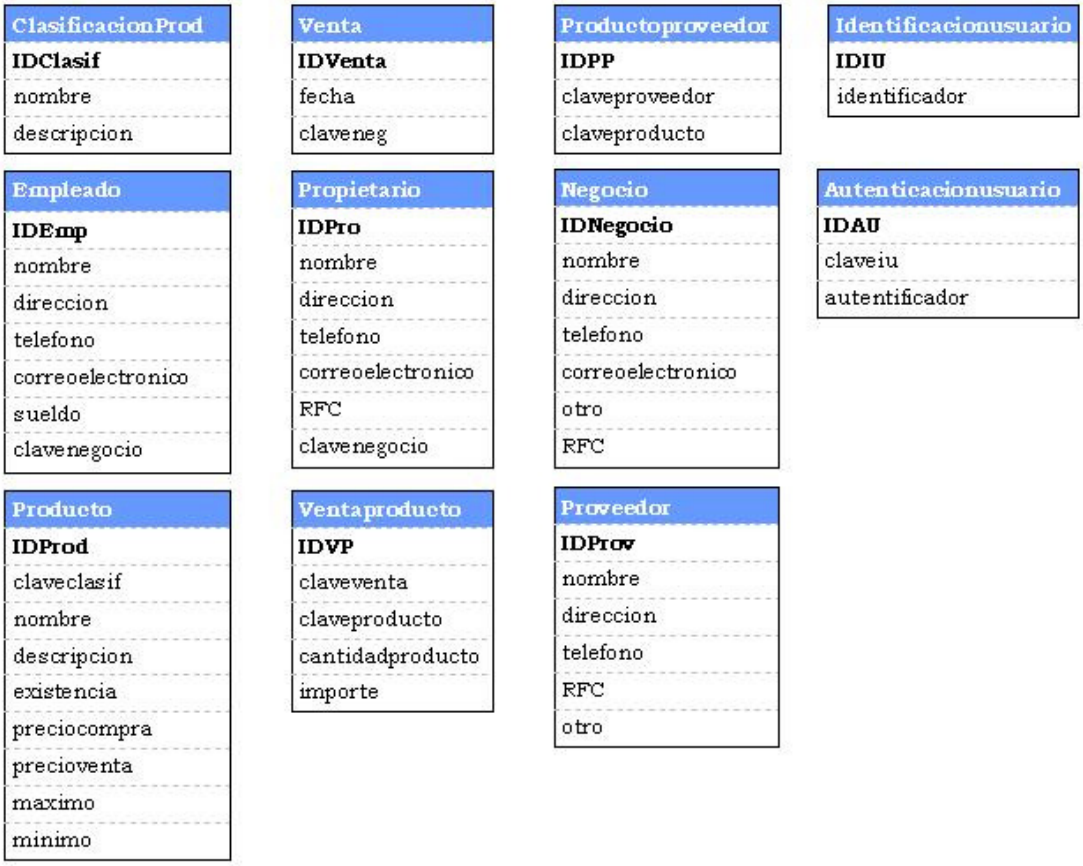
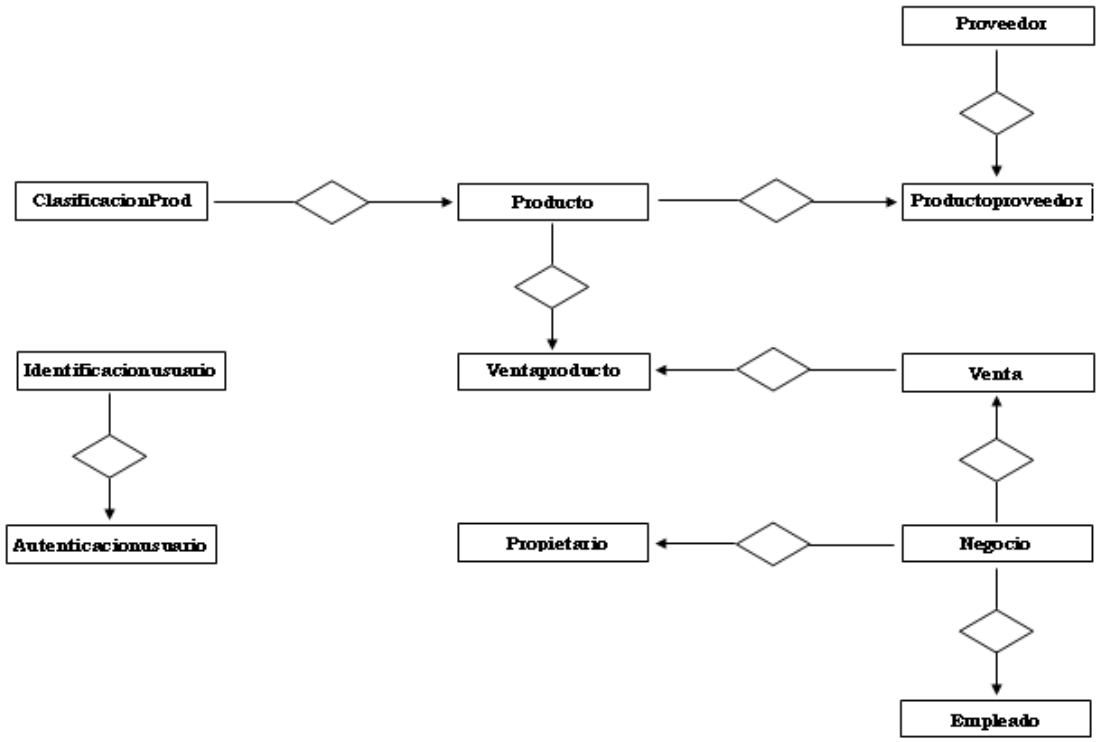


Fig. 5.2 Relaciones entre tablas



5.3.4 Pantallas del sistema de información

Las siguientes pantallas, son las que el sistema utilizará como interfaz con el usuario.

Cabe destacar que para la realización de estas pantallas, se utilizó el lenguaje de programación orientado a objetos Visual Basic.

A continuación se explicará el funcionamiento de cada pantalla.

5.3.4.1 Pantallas de seguridad

Las dos pantallas siguientes, son las que asignarán las concesiones específicas a cada tipo de usuario, es decir son la seguridad que se programo con el sistema de información realizado.

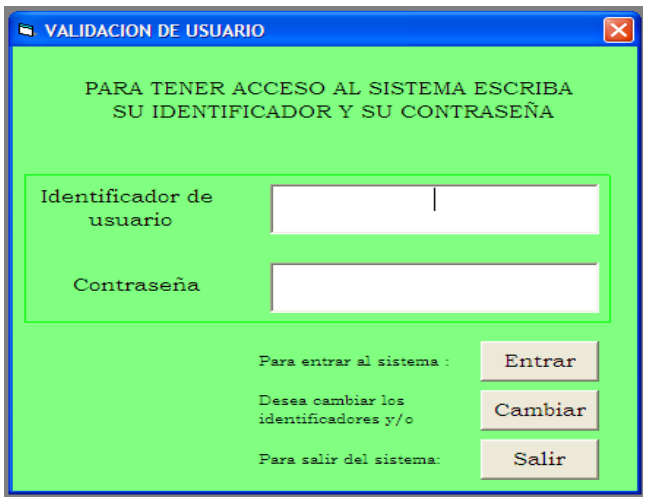


Fig. 5.3 Validación de Usuarios

La pantalla de la figura 5.3, es la primera que aparece al inicializar el sistema.

Esta, es una pantalla de seguridad que pedirá al usuario identificarse, y dependiendo del tipo de usuario que sea le dará concesiones especificas.

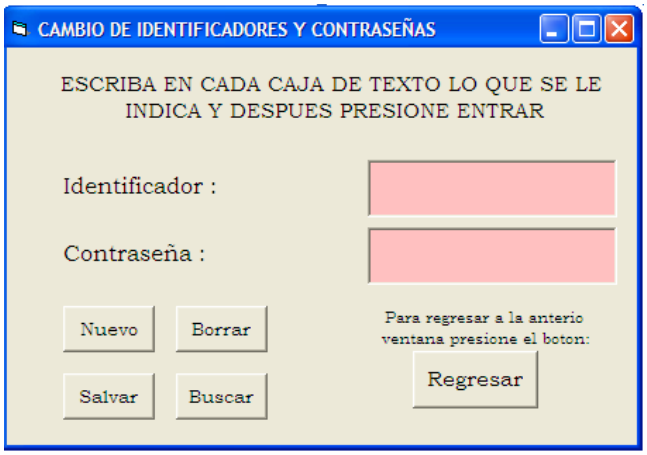


Fig. 5.4 Altas, bajas, cambios de usuarios

La figura 5.4 es la pantalla para la modificación, eliminación, consulta o adición de usuarios.

Esta pantalla solo estará disponible si el usuario es se identifica como administrador en la figura 5.3.

5.3.4.2 Pantallas de Datos

Al pulsar entrar en la pantalla de validación de usuario (Figura 5.3), se visualizara la pantalla de opciones (Figura 5.5), que es un menú que permitirá al usuario, elegir la acción que desee realizar.

Esta pantalla tiene cuatro menús: Catálogos, Ventas, Reportes, Salir.

Fig. 5.5 Menú de opciones-Catálogos

El menú de catálogos que contiene todas las pantallas que el sistema utiliza para introducir, modificar, borrar o buscar información (Figura 5.5).

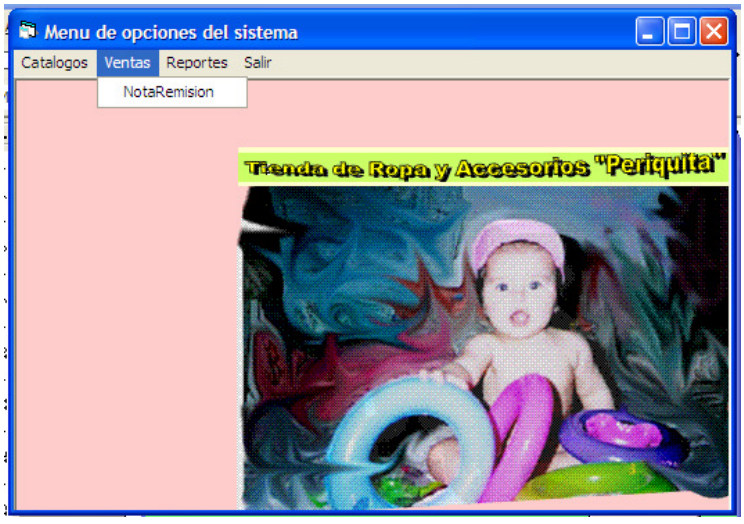


Fig. 5.6 Menú de opciones-Ventas

El menú ventas que contiene la pantalla que permitirá al sistema registrar cada venta que haga el negocio (Figura 5.6)

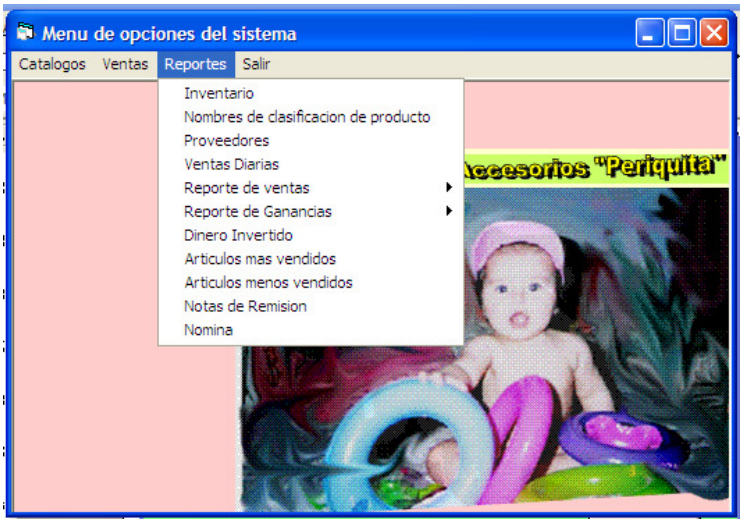


Fig. 5.7 Menú de opciones-Reportes

El menú reportes, que contendrá todos los reportes que es sistema realiza (Figura 5.7)

El menú salir que permitirá al usuario salir del sistema (No se presenta figura porque este menú no contiene submenús).

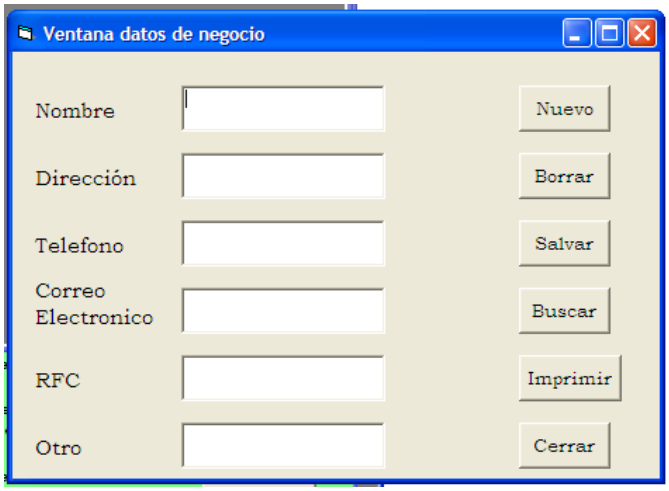


Fig. 5.8 Pantalla de captura de Negocio

Pantalla de la figura 5.8 que aparecerá al seleccionar la opción catálogo-negocio del menú principal.

Esta pantalla permite añadir, modificar, borrar o consultar los datos referentes al negocio.

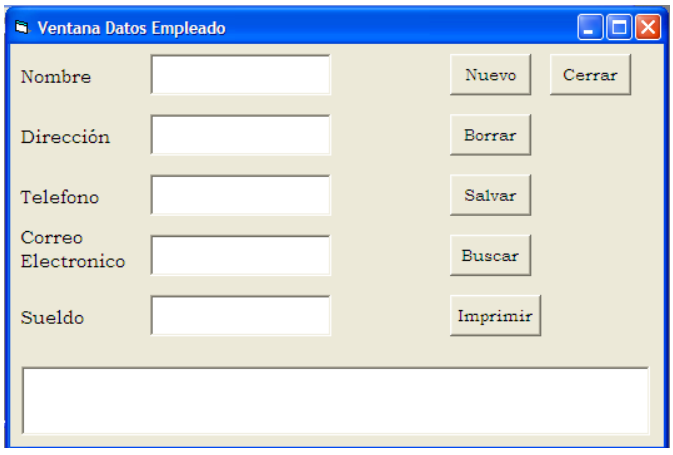


Fig. 5.9 Pantalla de captura de Empleados

Pantalla de la figura 5.9 que aparecerá al seleccionar la opción catálogo-Empleado del menú principal.

Esta pantalla permite añadir, modificar, borrar o consultar los datos referentes a los empleados.

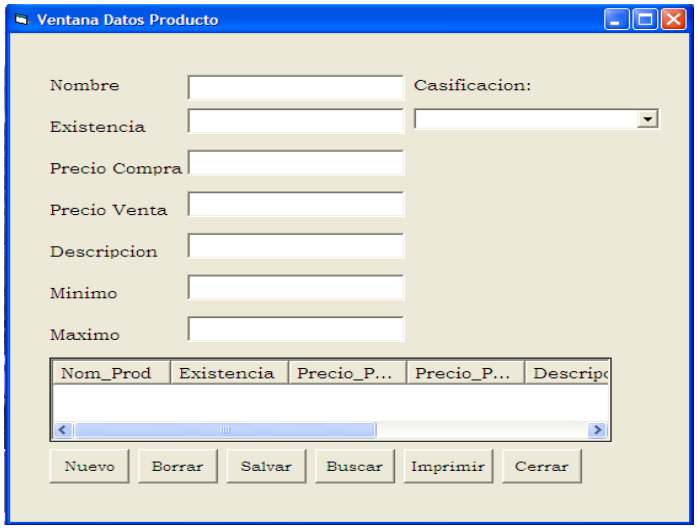


Fig. 5.10 Pantalla de captura de Productos

Pantalla de la figura 5.10 que aparecerá al seleccionar la opción catálogo-Producto del menú principal.

Esta pantalla permite añadir, modificar, borrar o consultar los datos de productos existentes o de nuevos productos.

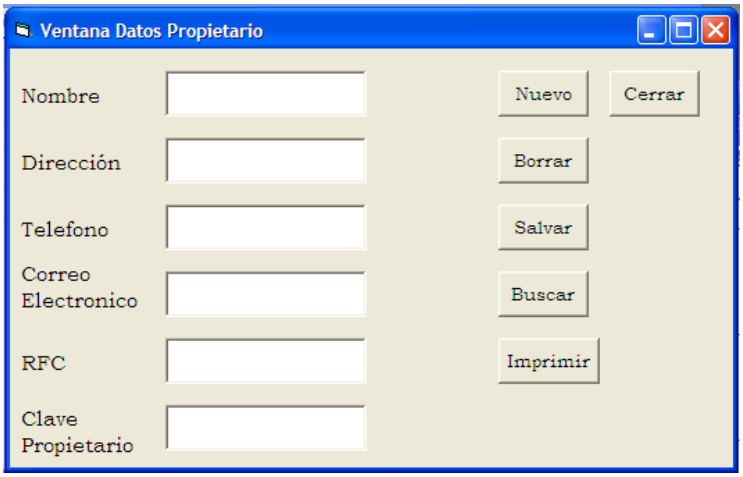


Fig. 5.11 Pantalla de captura de Propietario

Pantalla de la figura 5.11 que aparecerá al seleccionar la opción catálogo - propietario del menú principal.

Esta pantalla permite añadir, modificar, borrar o consultar los datos del propietario o propietarios del negocio.

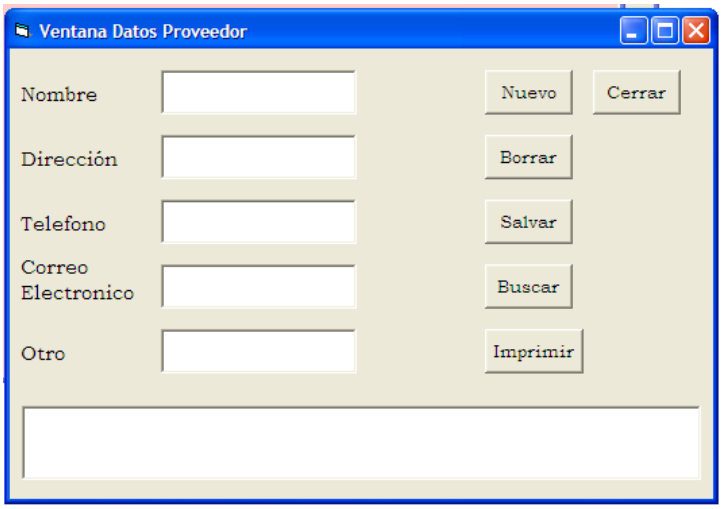


Fig. 5.12 Pantalla de captura de Proveedores

Pantalla de la figura 5.12 que aparecerá al seleccionar la opción catálogo-Proveedor del menú principal.

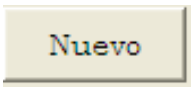
Esta pantalla permite añadir, modificar, borrar o consultar los datos referentes a los proveedores.

Fig. 5.13 Pantalla de captura de Ventas

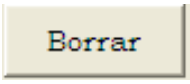
Pantalla de la figura 5.13 que aparecerá al seleccionar la opción venta-Nota de remisión del menú principal.

Esta pantalla permite añadir, modificar, borrar o consultar los datos especificados en la pantalla.

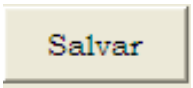
5.3.4.2.1 A cerca de los botones de mandato



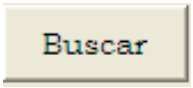
Este botón, permite añadir nuevos datos a la base de datos.



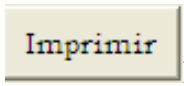
Este botón, permite borrar datos existentes en la base de datos.



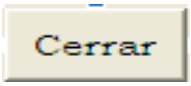
Este botón, permite modificar los datos de la base de datos y guardarlos nuevamente.



Este botón permite buscar datos en la base de datos.



Este botón, permite imprimir los datos que se visualizan en la pantalla.



El botón "Cerrar", permite cerrar la pantalla.

5.3.4.2.2 A cerca de las concesiones según el tipo de usuario

Como se sabe en este sistema existen dos tipos de usuarios, el administrador y los usuarios simples, cada uno de los cuales tiene concesiones diferentes que ya se explicaron anteriormente.

Cuando el usuario es el administrador, todos los botones de mandato estarán disponibles, es decir que ejecutarán las órdenes para las que fueron programados.

Cuando el usuario es simple, solo los botones siguientes estarán disponibles: nuevo, buscar, imprimir y cerrar.

5.3.4.3 Formato de Reportes

Cada reporte que elaborará este sistema, tendrá un formato específico. En este punto se mostrará, la forma que el sistema presentará los datos en cada uno de los reportes.

Fig. 5.14 Reporte de inventario

Nombre de Negocio								
Dirección del Negocio			Teléfono del Negocio			Fecha de elaboración del reporte		
Clave clasificación del artículo	Nombre clasificación del artículo	Clave artículo	Nombre del artículo	Precio compra	Precio venta	Máximo	Mínimo	Clave proveedor

Fig. 5.15 Reporte de nombres de clasificaciones de artículos

Nombre de Negocio			
Dirección del Negocio	Teléfono del Negocio	Fecha de elaboración del reporte	
Nombre clasificación de artículos	Clave clasificación de artículos	Clave artículo	Nombre artículo

Fig. 5.16 Reporte de proveedores

Nombre de Negocio					
Dirección del Negocio		Teléfono del Negocio		Fecha de elaboración del reporte	
Nombre proveedor	Dirección del proveedor	Teléfono del proveedor	RFC del proveedor	Clave clasificación de artículos que vende	Nombre del artículo

Fig. 5.17 Reportes de ventas diarias

Nombre de Negocio					
Dirección del Negocio		Teléfono del Negocio		Fecha de elaboración del reporte	
Nombre del artículo	Clave del artículo	Precio compra	Precio venta	Ganancias por tipo de artículo	Ganancias totales

Fig. 5.18 Reportes de ventas

Nombre de Negocio					
Dirección del Negocio		Teléfono del Negocio		Fecha de elaboración del reporte	
Día, mes ó año	Nombre del artículo	Clave del artículo	Precio unitario venta	Importe total por artículo	Importe total

Fig. 5.19 Reporte de ganancias

Nombre de Negocio							
Dirección del Negocio			Teléfono del Negocio		Fecha de elaboración del reporte		
Día, mes ó año	Nombre del artículo	Clave del artículo	Precio unitario venta	Precio unitario compra	Ganancia por unidad	Ganancia por tipo de artículo	Ganancias totales

Fig. 5.20 Reporte de dinero invertido

Nombre de Negocio									
Dirección del Negocio			Teléfono del Negocio		Fecha de elaboración del reporte				
Clave clasificación de artículo	Clave artículo	Nombre artículo	Número de artículos del mismo tipo en exixtencia	Precio unitario venta	Precio unitario compra	Total del mismo tipo de artículo venta	Total del mismo tipo de artículo compra	Total venta	Total compra

Fig. 5.21 Reporte de artículos más vendidos

Nombre de Negocio					
Dirección del Negocio		Teléfono del Negocio		Fecha de elaboración del reporte	
Nombre del artículo	Precio venta	Precio compra	Número de artículos vendidos	Clave proveedor	Nombre proveedor

Fig. 5.22 Reporte de artículos menos vendidos

Nombre de Negocio					
Dirección del Negocio		Teléfono del Negocio		Fecha de elaboración del reporte	
Nombre del artículo	Precio venta	Precio compra	Número de artículos vendidos	Clave proveedor	Nombre proveedor

Fig. 5.23 Notas de venta

Nombre de Negocio					
Dirección del Negocio		Teléfono del Negocio		Correo electrónico del reporte	
RFC del Negocio			Fecha de elaboración de la nota		
Número de folio					
Clave del artículo	Nombre del artículo	Precio por unidad	Cantidad	Importe	Total

Fig. 5.24 Nómina

Nombre de Negocio			
Dirección del Negocio	Teléfono del Negocio		Fecha de elaboración del reporte
Clave empleado	Nombre empleado	Número de folio venta	Importe total venta

A cerca de los Reportes

Los reportes solo podrán ser consultados cuando el usuario se identifique como el administrador.

5.4 Políticas de Seguridad

A partir de ahora y para más comodidad, nombraremos al propietario del negocio como administrador y a los empleados como usuarios simples.

En los siguientes puntos se describirán todas las normas que tendrá el negocio en cuanto a seguridad de la información para operar correctamente:

- Generales
  - Utilizar la computadora solo para el uso del sistema
  - No dejar solo el negocio, mientras se encuentre abierto
  - Dar a conocer las políticas de seguridad a cada nuevo usuario.

- Derechos de acceso al sistema
  - Nadie, excepto el desarrollador del sistema, tiene derecho a modificar la estructura del mismo.
  - El administrador, tiene acceso total a la información que contiene el sistema, no así a la estructura del mismo.

- El usuario simple solo puede consultar e introducir información al sistema, no así modificarla.

❖ identificadores y contraseñas

- Solo el administrador puede cambiar, borrar o modificar un identificador de usuario o una contraseña.
- Las contraseñas son únicas y privadas, por lo que no se pueden compartir. Ninguna otra persona (a excepción del administrador) debe de conocer la contraseña del usuario.
- El administrador, tiene la responsabilidad de cambiar las contraseñas en los siguientes dos casos: Es desempleado algún usuario simple y/o la contraseña de un usuario simple o del mismo administrador ya no es confidencial.
- El administrador tiene que asignarle una contraseña a cada nuevo usuario del sistema.
- No reutilizar una contraseña en un nuevo usuario.
- Ningún usuario simple debe de tratar de adivinar o robar la contraseña de otro usuario.

CONCLUSIONES

Con la realización de este trabajo se logró, destacar la importancia que tiene la seguridad en el acceso a los sistemas de información, agrupar y definir todas las medidas y políticas de seguridad necesarias para hacer un sistema de información seguro y confiable para quienes lo operan, pues si se llevan a la practica, se minimizara mucho el riesgo de robo, pérdida o manipulación indebida de la información que maneja el sistema, lo que generará confianza en la información que arroja el mismo, permitiendo al personal de las diferentes áreas de la empresa utilizar la información que proporciona el sistema para el beneficio de la propia empresa.

La seguridad en el acceso a los sistemas de información es básica para que una empresa pueda ser competitiva.

El nivel de seguridad en el acceso a un sistema de información está directamente relacionado con el nivel de confidencialidad del sistema de información que va a proteger, a mayor necesidad de confidencialidad mayor nivel de seguridad.

Para que un sistema de seguridad sea eficiente tiene que ser integral, es decir tiene que componerse de la seguridad física, la seguridad lógica, las políticas de seguridad de la empresa y la revisión periódica de la seguridad en el sistema de información y del propio sistema.

Con el sistema que se realizó a la par de esta tesis, se logró minimizar el riesgo de robo de la información, se logró hacer más competitivo el negocio debido al orden y la confiabilidad en sus procesos.

Aquí cabe mencionar que el mecanismo de seguridad que se instauró en el sistema para la tienda de ropa y accesorios periquita fue un sistema simple y básico para cualquier sistema, debido a que es un negocio pequeño que no puede ni necesita invertir en mecanismos de seguridad mas sofisticados.

BIBLIOGRAFÍA

- ✓ Anónimo, **Maximum Security**, Cuarta edición, Ed. SAMS, USA, 2002, 945 p.

- ✓ Senn, James A., **Análisis y diseño de sistemas de información**, Segunda edición, Ed. McGraw-Hill, Colombia, 2000, 942 p.

- ✓ Weiss, Barrett, Hausman, Kira, **Security +**, Primera edición, Ed. Tittel, USA, 2003, 484 p.

- ✓ Weber, Chan, Bahadur, Gary, **Privacy Defended** Protecting Yourself Online, Primera edición, Ed. QUE, USA, 2002, 699 p.

Otras Fuentes

- ✓ http://www.monografias.com/trabajos14/proyectos-sistem/proyectos-sistem.shtml
- ✓ http://www.csi.map.es/csi/silice/Seg2.html
- ✓ http://www.csi.map.es/csi/silice/Segurd4.html
- ✓ http://www.csi.map.es/csi/silice/Segurd6.html
- ✓ http://www.csi.map.es/csi/silice/Segurd4.html

- ✓ http://www.csi.map.es/csi/silice/Segurd9.html
- ✓ http://www.csi.map.es/csi/criterios/seguridad/index.html
- ✓ http://www.rediris.es/cert/doc/unixsec/node6.html
- ✓ http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
- ✓ http://www.segu-info.com.ar/logica/seguridadlogica.htm
- ✓ http://www.microsoft.com/latam/athome/security/privacy/password.mspx
- ✓ http://es.wikipedia.org/wiki/Contrase%C3%B1a
- ✓ http://es.wikipedia.org/wiki/Criptograf%C3%ADa