UNIVERSIDAD DE SOTAVENTO, A. C.

ESTUDIOS INCORPORADOS A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INFORMÁTICA

“SEGURIDAD INFORMÁTICA EN EL SISTEMA DE INFORMACIÓN DE UNA TIENDA DE AUTOSERVICIO”

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE

LICENCIADO EN INFORMÁTICA

PRESENTA:

ANGÉLICA FUENTES TORRES

ASESOR DE TESIS:

LIC. JUAN JOSÉ GUTIERREZ QUIROZ

COATZACOALCOS, VERACRUZ MARZO DEL 2007.

UNIVERSIDAD DE SOTAVENTO, A. C.

AGRADECIMIENTOS

A Dios:

Por haberme guiado por buen camino, por haberme ayudado a salir adelante y darme la paz que he necesitado en los momentos de angustia.

A mis Padres:

Por ser las personas más importantes para mí, por haberme otorgado la vida, por sus consejos, por preocuparse por mí y por estar junto a mí en todo momento.

A mis hermanos: Nely y Enrique:

Por que a pesar de nuestras diferencias siempre han estado junto a mí en cada momento, porque aun sin saberlo me han dado fortaleza y apoyo.

A mi Tío Mario:

Por ser mí amigo, un apoyo incondicional para mí, por darme consejos y estar conmigo siempre. Muchas Gracias.

Al Ing. Edgar E. Paxtian Ortiz:

Por sus consejos que me ayudaron mucho en la realización de este proyecto, por su paciencia y su tiempo otorgados.

Los primeros conceptos de seguridad se evidencian en los inicios de la escritura con los Sumerios (3000 A. C.) o el Código de Hammurabi (2000 A. C.). Homero, Cicerón y César han sido autores de obras en donde aparecen ciertos rasgos de la seguridad en la guerra y el gobierno, e inclusive en algunos capítulos de la Biblia también se aborda este tema.

Los descubrimientos arqueológicos marcan, sin duda, las más importantes pruebas de seguridad de los antiguos: las pirámides egipcias, el palacio de Sargon, el templo Karnak en el valle del Nilo; el dios egipcio Anubi representado con una llave en su mano, etc.

Se sabe que los primitivos, para evitar amenazas, reaccionaban con los mismos métodos defensivos de los animales: luchando o huyendo (fight or flight), para eliminar o evitar la causa. Así, la pugna por la vida se convertía en una parte esencial y los conceptos de alertar, evitar, detectar, alarmar y reaccionar, ya eran manejados por ellos.

Como todo concepto, la Seguridad se ha desarrollado y ha seguido una evolución dentro de las organizaciones sociales. La sociedad se conformó en familias, y esto se convirtió en un elemento limitante para huir. Se tuvieron que concebir nuevas estrategias de intimidación y disuasión para convencer al atacante que las pérdidas eran inaceptables contra las posibles ganancias.

En la informática, la “seguridad” es una característica de cualquier sistema que nos indica que está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro.

Para que un sistema se pueda definir como seguro debemos de dotar de tres características al mismo:

- Integridad
- Confidencialidad
- Disponibilidad

Dependiendo de las fuentes de amenazas, la seguridad puede dividirse en seguridad lógica y seguridad física, temas que serán abordados en el presente trabajo.

Precisamente la investigación está enfocada a la Seguridad en un Sistema de Información, basándonos específicamente en el Sistema Entec, el cual es utilizado en la Tienda de Autoservicio “Comercial La Fuente”.

En términos generales, se compone de siete capítulos, cuyo contenido se describe brevemente en los siguientes párrafos:

En el capítulo I se presentan los antecedentes de la empresa y sus características generales, incluyendo filosofía y estructura organizacional.

El planteamiento del problema en sí se expone en el capítulo II, el cual está divido en operación general de la empresa, riesgos físicos en el sistema, seguridad lógica y enunciación del problema.

En el capítulo III se desarrolla el marco teórico del trabajo de investigación, comprendiendo básicamente lo relacionado a la seguridad física y la seguridad lógica, la importancia que ambas tienen dentro de una empresa, sus amenazas y algunas recomendaciones para evitar daños en la misma.

En el capítulo IV se definen los objetivos tanto generales como específicos del trabajo de investigación, así como también se formula la hipótesis, la justificación del tema y el alcance del mismo.

En el capítulo V se especifica el diseño metodológico del trabajo de investigación, incluyendo la encuesta aplicada al personal que interactúa con el Sistema Entec, así como una breve explicación del tipo de encuesta empleada.

Los resultados de la encuesta aplicada a los empleados de “Comercial La Fuente” se muestran mediante gráficas en el capítulo VI, realizando una breve explicación de cada una de las gráficas; de igual manera se presentan los aspectos más relevantes de la entrevista efectuada al Administrador del Sistema Entec.

Y por último, en el capítulo VII, tenemos la conclusión de todo el trabajo de investigación, dando respuesta a la hipótesis planteada en el capítulo IV.

INTRODUCCIÓN

“COMERCIAL LA FUENTE “

I.1 FUNDACIÓN DE LA EMPRESA

El comienzo se dio en el año de 1982, cuando el Lic. Alejandro Mondragón Velásquez instaló la tienda de pinturas “IMPERMEX HUATULCO”, la cual se encargaba de distribuir pinturas a diversas empresas de la localidad; más adelante abre “Impermex” en el Puerto de Salina Cruz y otra más en Puerto Escondido, cerrando años más tarde estas últimas sucursales.

El 19 de Noviembre de 1986, viendo la necesidad que se tenía en Bahías de Huatulco, decide crear la ferretería “MEOSA, S.A. DE C. V.”, estableciendo una nueva fuente de empleos y satisfaciendo las necesidades de la localidad, misma empresa que se mantiene hasta la fecha.

Años después, crea y vende “Plaza Oaxaca” con 26 locales comerciales, la cual fue la primera en la localidad.

El día 15 de abril de 1991 crea en bahías de Huatulco la tienda de autoservicio “COMERCIAL LA FUENTE”. Proporcionando una gran variedad de productos de primera necesidad con la que no se contaba anteriormente, viendo la necesidad de expandir sus servicios, para satisfacer las necesidades se crean dos sucursales, una en el municipio de Pochutla en Noviembre de 1994 y otra en Santa María Huatulco el 13 Junio del 2003, quedando la de bahías de Huatulco como matriz.

En el año de 1996 crea Plaza Galerías con un Hotel “Amakal”, el cual vende más tarde (año 2004).

El 15 de Julio del 2003 se crea la sociedad de Plaza “El Madero”, teniendo como objetivo una plaza donde hubiera centros comerciales, restaurantes, centros recreativos de juegos de mesa y un cine para atraer un gran turismo; esto tiene como consecuencia más inversiones en Huatulco, la cual es inaugurada en Enero del 2004. Y para julio de 2006 inaugura una cuarta sucursal de “Comercial la Fuente” ubicada en el sector “T” de esta ciudad.

I.2 PRODUCTOS Y SERVICIOS

Actualmente, la empresa cuenta con una gran variedad de artículos de ferretería, pintura, impermeabilización, abarrotes, frutas y verduras a precios bajos y de alta calidad.

I.3 VENTAJAS COMPETITIVAS

- Gente capacitada en el área a desarrollar.
- Buen ambiente de trabajo
- Trabajo en equipo
- Precios justos
- Productos de buena calidad

I.4 POLÍTICAS:

- Se prohíbe el uso de shorts, sandalias, playeras sin mangas, aretes, gorras o cualquier otro accesorio que sea diferente al uniforme de la empresa.

- Queda prohibido comer dentro de cualquier área de trabajo, el consumo de alimentos queda restringido solo al área de comedor.

- Se prohíbe fumar dentro de las instalaciones de la empresa, teniendo la posibilidad de hacerlo únicamente en horas de comida.

- Quedan estrictamente prohibidas las rifas, venta de zapatos por catálogo o venta de cualquier artículo que sea ajeno a la empresa.

- Se prohíben las visitas de personas ajenas a la empresa en horarios de trabajo con fines personales.

- Se prohíben las llamadas telefónicas de índole personal.

- Se prohíbe el uso de lenguaje altisonante para dirigirse a los compañeros.

- Las mujeres deberán de cuidar que su maquillaje no sea exagerado, pero que permanezca debidamente presentable.

- Las mujeres tienen prohibido maquillarse durante el horario de trabajo.

- El respeto a las ideas es una base de esta empresa, por lo tanto, se debe de respetar a las demás personas sin ignorarlas o burlarse de ellas.

I.5 MISIÓN

- Ofrecer un mejor servicio de calidad a nuestros clientes, tanto internos como externos, desarrollando a nuestro personal y manteniendo principios de integridad, honestidad y respeto.

- Ser una empresa comprometida con la comunidad, preservación de medio ambiente y desarrollo de Bahías de Huatulco.

- Cumplir con los objetivos de rentabilidad de la Gerencia General.

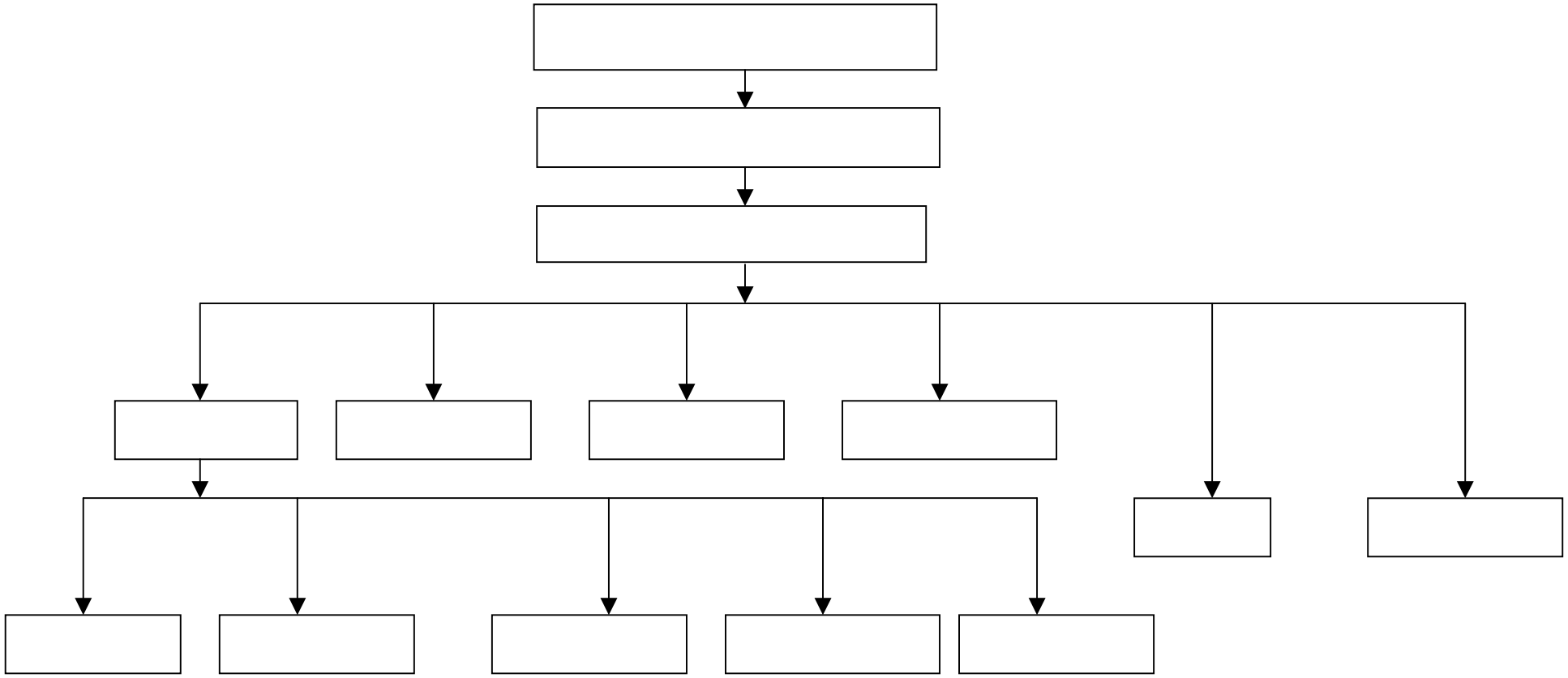
I.6 VISIÓN

Llegar a ser la mejor empresa que satisfaga las necesidades de nuestros clientes proporcionándoles una mejor calidad y servicio. Crecer de manera significativa hacia mercados locales siempre de la mano de nuestros empleados, que son la base fundamental de la empresa.

I.7 VALORES

- Honestidad
- Lealtad
- Actitud de servicio
- Respeto a la persona
- Austeridad
- Dedicación al trabajo
- Honradez

I.8 ESTRUCTURA EMPRESARIAL



I.9 BREVE DESCRIPCIÓN DE PUESTOS

DIRECTOR GENERAL:

Es la persona que ocupa el puesto principal dentro de la empresa ya que sobre este puesto recae toda la responsabilidad de la empresa y desde aquí se deben de tomar las decisiones que puedan afectar de manera directa a la empresa. Su principal función es la de vigilar el buen funcionamiento de la empresa.

GERENTE ADMINISTRATIVO:

Es la persona encargada de llevar la contabilidad de la empresa así como de administrar los bienes de la misma.

GERENTE DE OPERACIONES:

Es la persona encargada de la operación de la tienda de autoservicio matriz así como las diversas sucursales.

JEFE DE PISO:

Es la persona encargada de vigilar el buen desempeño del personal de la tienda matriz, así como también de atender a los clientes. De igual manera vigilar cada uno de los departamentos de la tienda para que siempre estén en óptimas condiciones y se cuente con los productos necesarios para la satisfacción de los clientes.

JEFE DE ABARROTES:

Es la persona encargada del Departamento de Abarrotes, su principal función es realizar un inventario de los productos que en dicho departamento

se exhiben, esto con la finalidad de mantener existencias, ya sea en la tienda o en almacén; tiene también a su cargo al personal que colabora en este mismo departamento a los cuales tiene que supervisar para que frenteen (acomoden) los productos día a día.

JEFE DE MERCANCÍAS GENERALES:

Es la persona encargada del Departamento de Mercancías Generales, su principal función es realizar un inventario de los productos que en dicho departamento se exhiben, esto con la finalidad de mantener existencias ya sea en la tienda o en almacén; tiene también a su cargo a personal que colabora en este mismo departamento a los cuales tiene que supervisar para que frenteen (acomoden) los productos día a día.

JEFA DE SALCHIHONERIA:

Es la persona encargada del Departamento de Salchichonería y del Departamento de Frutas y Verduras; su principal función es realizar un inventario de los productos que en dicho departamento se exhiben, esto con la finalidad de mantener existencias ya sea en la tienda o en almacén; tiene también a su cargo al personal que colabora en este mismo departamento a los cuales tiene que supervisar para que frenteen (acomoden) los productos día a día. También tiene que capacitar constantemente a su personal, ya que los productos que se manejan en este departamento son más delicados y requieren de refrigeración constante.

CAJERA GENERAL:

Es la persona encargada del área de cajas, supervisa el buen desempeño de las cajeras, realiza los cortes de caja durante el día, hace los depósitos bancarios y lleva el control de los horarios de las cajeras.

ENCARGADA DE COSTOS:

Es la persona encargada de dar de alta los productos en el sistema Entec, realiza reportes de mercancía recibida, faltantes y mercancía que llega en mal estado; da de alta las ofertas que se manejan cada fin de semana en la tienda, calcula los precios de los productos.

ENCARGADO DE SUCURSAL MADERO:

Es la persona encargada de vigilar la operación de la sucursal “El Madero”.

ENCARGADO DE SUCURSAL POCHUTLA:

Es la persona encargada de vigilar la operación de la sucursal Pochutla.

ENCARGADO DE SUCURSAL SANTA MARIA:

Es la persona encargada de vigilar la operación de la sucursal Santa María.

ENCARGADO DE ALMACÉN:

Es la persona encargada de recibir la mercancía en almacén, verificar el buen estado de la misma y organizarla dependiendo del departamento al que pertenezcan.

ENCARGADA DE FARMACIA:

Es la persona encargada de llevar un control de los medicamentos, el personal y horarios que se manejan en este departamento.

I.10 INSTALACIONES

Las instalaciones de esta tienda de autoservicio están ubicadas en el centro de Bahías de Huatulco, dichas instalaciones están divididas por departamentos ya que esto facilita la ubicación de los productos a los clientes.

La estructura de la tienda está en óptimas condiciones, esto debido a que ésta fue remodelada en Noviembre del 2004.

La iluminación, altura del techo y ventilación son las idóneas para este tipo de establecimientos.

Al llevar a cabo la remodelación de la tienda, ampliaron las instalaciones de la misma, cambiaron pisos y pintura; así como también la estructura del cableado; esto permite tener las instalaciones en óptimas condiciones.

I.11 RECURSOS TECNOLÓGICOS

La empresa se dedica principalmente a la venta de productos de primera necesidad, de ahí que para poder llevar a cabo las operaciones de venta de productos requiera de un sistema que le permita controlar las ventas originadas durante el día, así como también que imprima un comprobante de venta en el cual el cliente pueda corroborar lo que esta comprando y el precio en que lo compró.

Estas son las principales necesidades que la empresa desea resolver con un sistema apto para su giro, pero no son las únicas, ya que también tiene que ofertar productos, hacer cancelaciones, imprimir reportes de ventas por cajera y por horario, así como establecer un vínculo para el Departamento Contable.

El sistema Entec le ofrece resolver la mayor parte de estas necesidades, ya que es un sistema muy completo y está diseñado precisamente para empresas de este giro.

I.12 DESCRIPCIÓN DEL SISTEMA ENTEC

El sistema de facturación Entec Retail es una herramienta de software pensada para integrar el proceso de venta minorista / mayorista con la base de datos de la empresa.

Este sistema permite el registro de las transacciones de ventas de bienes o servicios y la cobranza por parte de terceros, respetando las normas legales e impositivas. El sistema está orientado a su utilización en puntos de venta autónomos o interconectados, en redes de área local o redes de área extendida (standalone/LAN/WAN), o mediante conexión asincrónica (correo electrónico/medios magnéticos). Por su alta flexibilidad, permite la integración de múltiples negocios con el mismo software: venta minorista en autoservicios, supermercados e hipermercados, venta mayorista, farmacias, ópticas, laboratorios de revelado, patios de comida, restaurantes, juegos, etc.

El Entec Retail Punto de Venta se basa en una filosofía de base de datos distribuida a nivel de empresa. Los datos comerciales de los artículos involucrados en el proceso comercial (precios, costos, condiciones de compra, los datos logísticos y de abastecimiento, la información operativa, la información de los clientes, las transacciones en las cajas y la estadística de ventas) son manejados en una base de datos central que actualiza la información del sistema en cada sucursal. Los precios de los artículos se pueden administrar de forma centralizada y permitir o no modificaciones en las bocas o puntos de venta. Estos puntos de venta acceden en tiempo real a una copia de la base de datos de la empresa tomando toda la información de la misma fuente donde se genera. Esta base de datos se puede convertir en el

centro del resto de los sistemas de soporte de venta para lograr que todos los precios que se presentan en una sucursal (balanzas, cajas, etiquetas, carteles, terminales de consulta) sean obtenidos del mismo lugar sin posibilidad de diferencias.

El soporte de la información es un motor de base de datos relacional y el Entec Retail soporta a los líderes de la industria (Oracle, Sybase, Informix, Microsoft SQL Server) de manera nativa. También es posible utilizar cualquier base de datos con drivers ODBC que garantice consistencia transaccional. La filosofía del sistema es entonces la utilización de una arquitectura cliente/servidor para la integración de la facturación con el resto de los sistemas de la empresa utilizando las tecnologías líderes de bases de datos relacionales distribuidas.

El Sistema de facturación cliente/servidor para Windows está orientado a puntos de venta de locales gastronómicos con pantallas sensibles al tacto (TouchScreen) y teclados programables o tradicionales. Permite operar como un sistema de adición con mesas abiertas o en modalidad de facturación directa para patios de comidas. El operador puede seleccionar la mesa en un plano digital y luego elegir los productos a adicionar de un menú gráfico con fotos que se presentan en la pantalla.

Permite coordinar desde un único lugar las actualizaciones de parámetros de ventas, promociones, políticas comerciales, de seguridad y de auditoria. Concentra de todas las bocas la información de venta, existencias, excepciones, cobranzas de servicios, cuentas corrientes y fidelidad de clientes.
El programa de facturación se complementa con un sistema administrativo denominado Entec Retail Backoffice que permite el manejo de la información de ventas, cuentas corrientes de clientes, stock, tesorería, compras y proveedores.

En conjunto con Entec Retail Punto de Venta, se instala un complemento denominado Entec Retail Backoffice, el cual permite la administración de los datos del punto de venta. Este programa permite definir productos, clientes, medios de pago, operadores, listas de precios, promociones, documentos, etc. Además permite controlar las cuentas corrientes de clientes, el stock de los productos y emitir todo tipo de informes sobre la gestión de ventas.

Existen varias versiones del producto Entec Retail Backoffice, de acuerdo al tipo de actividad del usuario, la distribución geográfica de sus puntos de venta y su volumen de operaciones.

PLANTEAMIENTO DEL PROBLEMA

II.1 OPERACIÓN GENERAL DE LA EMPRESA

El conjunto de actividades que hacen posible el funcionamiento de la empresa exige un mecanismo que permita garantizar el registro de las operaciones con una eficiencia máxima.

Para una mejor comprensión de lo expresado con anterioridad, procederé a describir la interacción del personal con el Sistema de Información:

El sistema es ocupado principalmente en el área de cajas, motivo por el cual las cajeras son las principales personas que interactúan con dicho sistema:

- La encargada de costos maneja de forma directa la base de datos del sistema, ya que es la encargada de dar entrada a los productos que se reciben día a día para llevar actualizado el inventario de la tienda, a su vez calcula los precios de los productos con los que serán dados de alta en el sistema para su venta, esto lo hace tomando como referencia el precio que le fijan los proveedores en las facturas.

- Los jefes de área como son: jefe de piso, jefe de abarrotes, jefe de mercancías generales y la cajera general, son las personas que están facultadas para autorizar las cancelaciones, ofertas y devoluciones de los productos desde el sistema.

- Y por último, el administrador del sistema, quien es la persona encargada de vigilar el buen funcionamiento del mismo, así como de estar al pendiente de cualquier incidente que pueda ocurrir con el mismo y corregirlo a la brevedad para que ello no afecte el funcionamiento de la empresa.

II.2 RIESGOS FÍSICOS EN EL SISTEMA

Las instalaciones de la empresa son aptas para el giro al que se dedica, el área de cajas se encuentra ubicada en la entrada/salida de la tienda de autoservicio, contando con un equipo conformado por un cpu, monitor y teclado, los cuales se encuentran, aparentemente, en buenas condiciones y tienen una buena instalación; el área de costos se encuentra ubicado a un costado del almacén general, esto debido a que en almacén se recibe físicamente la mercancía que llevan los diferentes proveedores con los que cuenta la empresa y en el departamento de costos se hace la recepción electrónica de mercancía. Por último, el departamento de sistemas se encuentra ubicado en la planta alta de la empresa, desde ahí el administrador del sistema vigila el funcionamiento del mismo.

II.3 SEGURIDAD LÓGICA

Antes de comenzar a administrar la seguridad del sistema, se deben definir un conjunto de parámetros que establecen diferentes reglas en lo relacionado a los operadores y la seguridad, esto es, definir si para poder accesar al sistema se usarán contraseñas, la longitud mínima con que contará la clave de los operadores, la cantidad de días a los que vence la clave, la cantidad de cambios de clave que deben transcurrir para que el sistema permita utilizar nuevamente una clave, si las claves se pueden ingresar en mayúsculas o minúsculas, la cantidad de intentos de acceso en los que el sistema bloquea automáticamente la cuenta de un operador, entre otros parámetros que se irán definiendo dependiendo de los requerimientos de la operación de la empresa.

Uno de los problemas que se nos presentan en el Sistema Entec es el libre acceso que tiene el personal del Centro Comercial a dicho sistema; por ello se

requiere implementar medidas de seguridad en la información y en los procesos que se manejan en el Sistema Entec.

A continuación mencionaremos los procesos a los cuales no debe existir libre acceso por parte del personal del Centro Comercial:

- Acceso a entrada de datos al sistema (Altas, modificaciones y bajas de productos)
- Aplicación de Ofertas
- Cancelación de Productos
- Aprobación de Descuentos a Clientes
- Acceso al proceso de venta
- Acceso a los reportes diarios de ventas

Cualquier persona que quiera utilizar el Sistema ENTEC Retail Punto de Venta o el ENTEC Retail Backoffice, previamente debe ingresar su nombre de usuario y contraseña. Para que una persona tenga asignado un nombre de usuario y una contraseña, debe ser dada de alta como usuario en el ENTEC Retail Backoffice. En el momento de ingresar un nuevo usuario, se establece el grupo de usuario al que pertenece, su nombre de usuario y su contraseña. Los grupos de usuario se diferencian entre sí por las funciones que cumplen dentro de la empresa, esto es: Administradores, Operadores, Supervisores.

Se puede controlar a los usuarios del sistema, permitiendo o prohibiendo el uso de determinadas funciones dentro del mismo. De esta forma, el administrador asigna permisos a los usuarios para utilizar solo aquellas funciones del sistema que le corresponden, impidiendo el acceso a todas las restantes.

II.4 ENUNCIACIÓN DEL PROBLEMA

De manera general, es necesario verificar las condiciones de Operación del Sistema, desde las instalaciones, el equipo y hasta el manejo del propio sistema.

Esto nos permitirá determinar el grado de Seguridad Física y Lógica del Sistema; puesto que de ello depende el buen funcionamiento de la tienda de autoservicio.

MARCO TEÓRICO

Y

DE REFERENCIA

III.1 SEGURIDAD

La seguridad es como definimos la calidad de algo seguro, por tanto la seguridad de un sistema informático estará fijada por todos los elementos que lo componen en software y hardware.

La seguridad a nivel informático no se limitará entonces, por ejemplo, a la posibilidad de evitar la adulteración de la información o intromisión no autorizada a lugares restringidos de acceso; sino también a que los equipos donde se opera y almacena la información sean confiables, siendo la seguridad general establecida, tan buena como la menor seguridad de cualquier componente.

Se suele definir Seguridad Informática como el *"Conjunto de procedimientos que nos permite que nuestros datos de hoy puedan ser utilizados mañana sin ninguna merma de calidad en los mismos"*[1].[1]

III.2 SEGURIDAD FISICA

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos, hackers, virus, etc.; la seguridad de la misma será nula si no se ha previsto cómo combatir un incendio.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros no, tales como la detección de un atacante interno a

[1] Piratas Cibernéticos Cyberwars, Seguridad Informática e Internet, De Marcelo Rodao Jesús

la empresa que intenta acceder físicamente a una sala de operaciones de la misma.

Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.

Para algunos autores, la Seguridad Física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

III.2.1 AMENAZAS EN LAS INSTALACIONES

La seguridad física está enfocada a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales, tormentas e inundaciones.

2. Amenazas ocasionadas por el hombre.

3. Disturbios, sabotajes internos y externos deliberados.

No hace falta recurrir a películas de espionaje para sacar ideas de cómo obtener la máxima seguridad en un sistema informático, además de que la solución sería extremadamente cara. A veces basta recurrir al sentido común para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno.

A continuación se analizan los peligros más importantes que se corren en un centro de procesamiento; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

III.2.1.1 DESASTRES NATURALES

INCENDIOS

Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas.

Desgraciadamente los sistemas antifuego dejan mucho que desear, causando casi igual daño que el propio fuego, sobre todo a los elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputo.

Los diversos factores a contemplar para reducir los riesgos de incendio a los que se encuentra sometido un centro de cómputo son:

1. El área en la que se encuentran las computadoras debe estar en un local que no sea combustible o inflamable.

2. El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.

3. Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.

4. Debe construirse un “falso piso” instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.

5. No debe estar permitido fumar en el área de proceso.

6. Deben emplearse muebles incombustibles, y cestos metálicos para papeles. Deben evitarse los materiales plásticos e inflamables.

7. El piso y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos, deben ser impermeables.

SEGURIDAD DEL EQUIPAMIENTO

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es

necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

Para protegerlos se debe tener en cuenta que:

- La temperatura no debe sobrepasar los 18º C y el límite de humedad no debe superar el 65% para evitar el deterioro.
- Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

RECOMENDACIONES

El personal designado para usar extinguidores de fuego debe ser entrenado en su uso.

Si hay sistemas de detección de fuego que activan el sistema de extinción, todo el personal de esa área debe estar entrenado para no interferir con este proceso automático.

Implementar paredes protectoras de fuego alrededor de las áreas que se desea proteger del incendio que podría originarse en las áreas adyacentes.

Proteger el sistema contra daños causados por el humo, en particular, cuando sea espeso, negro y de materiales especiales, ya que puede ser muy dañino y requiere una lenta y costosa operación de limpieza.

INUNDACIONES

Se les define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputos.

Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.

Para evitar este inconveniente se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.

CONDICIONES CLIMATOLÓGICAS

Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada.

La frecuencia y severidad de su ocurrencia deben tomarse en cuenta al decidir la construcción de un edificio. La comprobación de los informes

climatológicos o la existencia de un servicio que notifique la proximidad de una tormenta severa, permite que se tomen precauciones adicionales, tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia.

TERREMOTOS

Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan; o muy intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas. El problema es que en la actualidad, estos fenómenos están ocurriendo en lugares donde no se los asociaba. Por fortuna los daños en las zonas improbables suelen ser ligeros.

III.2.1.2 AMENAZAS OCASIONADAS POR EL HOMBRE

SEÑALES DE RADAR

La influencia de las señales o rayos de radar sobre el funcionamiento de una computadora ha sido estudiada, exhaustivamente, desde hace varios años. Los resultados de las investigaciones más recientes son que las señales muy fuertes de radar pueden inferir en el procesamiento electrónico de la información, pero únicamente si la señal que alcanza el equipo es de 5 volts/metro, o mayor. Ello podría ocurrir sólo si la antena respectiva fuera visible desde una ventana del centro de procesamiento respectivo y, en algún momento, estuviera apuntando directamente hacia dicha ventana.

INSTALACIÓN ELÉCTRICA

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta una de las principales áreas a considerar en la seguridad física. Además, es una problemática que abarca desde el usuario hogareño hasta la gran empresa.

En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

PICOS Y RUIDOS ELECTROMAGNÉTICOS

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

CABLEADO

Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxial o la fibra óptica. Algunos edificios de oficinas ya se construyen con los cables instalados para evitar el tiempo y el gasto posterior, y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental.

Los riesgos más comunes para el cableado se pueden resumir en los siguientes:

1. **Interferencia:** estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada, por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración (de los datos que viajan a través de él) por acción de campos eléctricos, que sí sufren los cables metálicos.

2. **Corte del cable:** la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.

3. **Daños en el cable:** los daños normales con el uso pueden dañar el apantallamiento que preserva la integridad de los datos transmitidos o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables.

En la mayor parte de las organizaciones, estos problemas entran dentro de la categoría de daños naturales. Sin embargo, también se pueden ver como un medio para atacar la red si el objetivo es únicamente interferir en su funcionamiento.

SISTEMA DE AIRE ACONDICIONADO

Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras y equipos de proceso de datos en forma exclusiva.

Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, es recomendable instalar redes de

protección en todo el sistema de cañería al interior y al exterior, detectores y extintores de incendio, monitores y alarmas efectivas.

EMISIONES ELECTROMAGNÉTICAS

Desde hace tiempo se sospecha que las emisiones, de muy baja frecuencia que generan algunos periféricos, son dañinas para el ser humano. Según recomendaciones científicas estas emisiones podrían reducirse mediante filtros adecuados al rango de las radiofrecuencias, siendo estas totalmente seguras para las personas. Para conseguir que las radiaciones sean mínimas hay que revisar los equipos constantemente y controlar su envejecimiento.

AMBIENTE LUMINOSO

La iluminación es un factor decisivo para determinar la productividad en las empresas; con una iluminación deficiente, el rendimiento disminuye y esto se traduce a futuro en un gasto energético excesivo. Adicionalmente, en el personal se pueden presentar dolores de cabeza y afectaciones en los ojos.

AMBIENTE CLIMÁTICO

En cuanto al ambiente climático, la temperatura de una oficina con computadoras debe estar comprendida entre 18 y 21 grados centígrados y la humedad relativa del aire debe estar comprendida entre el 45% y el 65%. En todos los lugares hay que contar con sistemas que renueven el aire periódicamente. No menos importante es el ambiente sonoro, por lo que se recomienda no adquirir

equipos que superen los 55 decibeles, sobre todo cuando trabajan muchas personas en un mismo espacio.

III.2.1.3 DISTURBIOS, SABOTAJES INTERNOS Y EXTERNOS DELIBERADOS

ROBO

Las computadoras son posesiones valiosas de las empresas y están expuestas de la misma forma que lo están las piezas de stock e incluso el dinero. Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina. La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora. El software es una propiedad muy fácilmente sustraíble y las cintas y discos son fácilmente copiados sin dejar ningún rastro.

FRAUDE

Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines.

Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones.

SABOTAJE

El peligro más temido en los centros de procesamiento de datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

Físicamente, los imanes son las herramientas a las que se recurre, ya que con una ligera pasada la información desaparece, aunque las cintas estén almacenadas en el interior de su funda de protección. Una habitación llena de cintas puede ser destruida en pocos minutos y los centros de procesamiento de datos pueden ser destruidos sin entrar en ellos. Además, suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado. Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

CONTROL DE ACCESOS

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

III.2.1.4 UTILIZACIÓN DE GUARDIAS

CONTROL DE PERSONAS

El Servicio de Vigilancia es el encargado del control de acceso de todas las personas al edificio. Este servicio es el encargado de colocar los guardias en lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal.

A cualquier personal ajeno a la planta se le solicitará completar un formulario de datos personales, los motivos de la visita, hora de ingreso y de egreso, etc.

El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal a los distintos sectores de la empresa.

En este caso, la persona se identifica por algo que posee, por ejemplo una tarjeta de identificación. Cada una de ellas tiene un PIN (Personal Identification Number) único, siendo éste el que se almacena en una base de datos para su posterior seguimiento, si fuera necesario. Su mayor desventaja es que estas tarjetas pueden ser copiadas, robadas, etc., permitiendo ingresar a cualquier persona que la posea.

Estas credenciales se pueden clasificar de la siguiente manera:

- Normal o definitiva: para el personal permanente de planta.
- Temporaria: para personal recién ingresado.

- Contratistas: personas ajenas a la empresa, que por razones de servicio deben ingresar a la misma.
- Visitas.

Las personas también pueden acceder mediante alguna clave (por ejemplo un número de identificación o un password) que se solicitará a su ingreso. Al igual que el caso de las tarjetas de identificación, los datos ingresados se contrastarán contra una base donde se almacenan los datos de las personas autorizadas. Este sistema tiene la desventaja que generalmente se eligen identificaciones sencillas, bien se olvidan dichas identificaciones o incluso las bases de datos pueden verse alteradas o robadas por personas no autorizadas.

DESVENTAJAS DE LA UTILIZACIÓN DE GUARDIAS

La principal desventaja de la aplicación de personal de guardia es que éste puede llegar a ser sobornado por un tercero para lograr el acceso a sectores donde no esté habilitado, así como para poder ingresar o egresar de la planta con materiales no autorizados. Esta situación de soborno es muy frecuente, por lo que es recomendable la utilización de sistemas biométricos para el control de accesos.

SEGURIDAD CON ANIMALES

Sirven para grandes extensiones de terreno, y además tienen órganos sensitivos mucho más sensibles que los de cualquier dispositivo y, generalmente, el costo de cuidado y mantenimiento se disminuye considerablemente utilizando este tipo de sistema. Así mismo, este sistema posee la desventaja de que los animales pueden ser engañados para lograr el acceso deseado.

CONTROL DE VEHÍCULOS

Para controlar el ingreso y egreso de vehículos, el personal de vigilancia debe asentar en una planilla los datos personales de los ocupantes del vehículo, la marca y patente del mismo, y la hora de ingreso y egreso de la empresa.

III.2.1.5 UTILIZACION DE EQUIPOS ESPECIALES

UTILIZACIÓN DE DETECTORES DE METALES

El detector de metales es un elemento sumamente práctico para la revisión de personas, ofreciendo grandes ventajas sobre el sistema de palpación manual.

La sensibilidad del detector es regulable, permitiendo de esta manera establecer un volumen metálico mínimo, a partir del cual se activará la alarma.

La utilización de este tipo de detectores debe hacerse conocer a todo el personal. De este modo, actuará como elemento disuasivo.

HUELLA DIGITAL

Basado en el principio de que no existen dos huellas dactilares iguales, este sistema viene siendo utilizado desde el siglo pasado con excelentes resultados.

Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos, etc. (llamados minucias) características y la posición relativa de cada una de ellas es lo analizado para establecer la identificación de una persona. Está aceptado que dos

personas no tienen más de ocho minucias iguales y cada una posee más de 30, lo que hace al método sumamente confiable.

PROTECCIÓN ELECTRÓNICA

Se llama así a la detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas. Estas centrales tienen conectadas los elementos de señalización que son los encargados de hacerles saber al personal de una situación de emergencia. Cuando uno de los elementos sensores detectan una situación de riesgo, éstos transmiten inmediatamente el aviso a la central; ésta procesa la información recibida y ordena en respuesta la emisión de señales sonoras o luminosas alertando de la situación.

BARRERAS INFRARROJAS Y DE MICRO–ONDAS

Transmiten y reciben haces de luces infrarrojas y de micro–ondas respectivamente. Se codifican por medio de pulsos con el fin de evadir los intentos de sabotaje. Estas barreras están compuestas por un transmisor y un receptor de igual tamaño y apariencia externa. Cuando el haz es interrumpido, se activa el sistema de alarma, y luego vuelve al estado de alerta. Estas barreras son inmunes a fenómenos aleatorios como calefacción, luz ambiental, vibraciones, movimientos de masas de aire, etc.

Las invisibles barreras fotoeléctricas pueden llegar a cubrir áreas de hasta 150 metros de longitud (distancias exteriores). Pueden reflejar sus rayos por medio de espejos infrarrojos con el fin de cubrir con una misma barrera diferentes sectores.

Las micro–ondas son ondas de radio de frecuencia muy elevada. Esto permite que el sensor opere con señales de muy bajo nivel sin ser afectado por otras emisiones de radio, ya que están muy alejadas en frecuencia.

Debido a que estos detectores no utilizan aire como medio de propagación, poseen la ventaja de no ser afectados por turbulencias de aire o sonidos muy fuertes.

Otra ventaja importante es la capacidad de atravesar ciertos materiales como son el vidrio, lana de vidrio, plástico, tabiques de madera, revoques sobre madera, mampostería y hormigón.

DETECTOR ULTRASÓNICO

Este equipo utiliza ultrasonidos para crear un campo de ondas. De esta manera, cualquier movimiento que realice un cuerpo dentro del espacio protegido, generará una perturbación en dicho campo que accionará la alarma. Este sistema posee un circuito refinado que elimina las falsas alarmas. La cobertura de este sistema puede llegar a un máximo de 40 metros cuadrados.

DETECTORES PASIVOS SIN ALIMENTACIÓN

Estos elementos no requieren alimentación extra de ningún tipo, sólo van conectados a la central de control de alarmas para mandar la información de control. Los siguientes están incluidos dentro de este tipo de detectores:

1. Detector de aberturas: contactos magnéticos externos o de embutir.

2. **Detector de roturas de vidrios:** inmune a falsas alarmas provocadas por sonidos de baja frecuencia; sensibilidad regulable.
3. **Detector de vibraciones:** detecta golpes o manipulaciones extrañas sobre la superficie controlada.

SONORIZACIÓN Y DISPOSITIVOS LUMINOSOS

Dentro de los elementos de sonorización se encuentran las sirenas, campanas, timbres, etc. Algunos dispositivos luminosos son los faros rotativos, las balizas, las luces intermitentes, etc. Estos deben estar colocados de modo que sean efectivamente oídos o vistos por aquellos a quienes están dirigidos. Los elementos de sonorización deben estar bien identificados para poder determinar rápidamente si el estado de alarma es de robo, intrusión, asalto o aviso de incendio.

Se pueden usar transmisores de radio a corto alcance para las instalaciones de alarmas locales. Los sensores se conectan a un transmisor que envía la señal de radio a un receptor conectado a la central de control de alarmas encargada de procesar la información recibida.

CIRCUITOS CERRADOS DE TELEVISIÓN

Permiten el control de todo lo que sucede en las instalaciones según lo captado por las cámaras estratégicamente colocadas. Los monitores de estos circuitos deben estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista (para ser utilizada como medida disuasiva) u ocultas (para evitar que el intruso sepa que está siendo captado por el personal de seguridad).

Todos los elementos anteriormente descritos poseen un control contra sabotaje, de manera que si en algún momento se corta la alimentación o se produce la rotura de alguno de sus componentes, se enviará una señal a la central de alarma para que ésta accione los elementos de señalización correspondientes.

EDIFICIOS INTELIGENTES

La infraestructura inmobiliaria no podía quedarse rezagada en lo que se refiere a avances tecnológicos.

El Edificio Inteligente (surgido hace unos 10 años) se define como una estructura que facilita a usuarios y administradores, herramientas y servicios integrados a la administración y comunicación. Este concepto propone la integración de todos los sistemas existentes dentro del edificio, tales como teléfonos, comunicaciones por computadora, seguridad, control de todos los subsistemas del edificio (gas, calefacción, ventilación y aire acondicionado, etc.) y todas las formas de administración de energía.

Una característica común de los Edificios Inteligentes es la flexibilidad que deben tener para asumir modificaciones de manera conveniente y económica.

III.3 SEGURIDAD LÓGICA

Luego de ver cómo nuestro sistema puede ser afectado por la falta de Seguridad Física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos, sino contra la información por él almacenada y procesada.

Así, la Seguridad Física sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren; estas técnicas las brinda la Seguridad Lógica.

Es decir, que la Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean serán:

1. Restringir el acceso a los programas y archivos.

2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.

3. Asegurar que se estén utilizando los datos, archivos y programas correctos en/y por el procedimiento correcto.

4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.

5. Que la información recibida sea la misma que ha sido transmitida.

6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.

7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

III.3.1 CONTROLES DE ACCESO

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. Al respecto, el National Institute for Standars and Technology (NIST) ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

IDENTIFICACIÓN Y AUTENTIFICACIÓN

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina Identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación.

Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

1. Algo que solamente el individuo conoce; por ejemplo: una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.

2. Algo que la persona posee; por ejemplo: una tarjeta magnética.

3. Algo que el individuo es y que lo identifica unívocamente; por ejemplo: las huellas digitales o la voz.

4. Algo que el individuo es capaz de hacer; por ejemplo: los patrones de escritura.

Para cada una de estas técnicas vale lo mencionado en el caso de la seguridad física, en cuanto a sus ventajas y desventajas. Se destaca que en los

dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan; mientras que por otro lado, los controles de autenticación biométricos serían los más apropiados y fáciles de administrar, resultando ser también, los más costosos por lo dificultosos de su implementación eficiente.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina "single log–in" o sincronización de passwords.

Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un servidor de autenticaciones sobre el cual los usuarios se identifican, y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder. Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas.

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos. Esta administración abarca:

1. Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus

requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.

2. Además, la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.

3. Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos. Las mismas deben encararse desde el punto de vista del sistema operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoria o por la gerencia propietaria del sistema; siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera de acuerdo con sus funciones.

4. Las revisiones deben orientarse a verificar la adecuación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso. Para esto, deben analizarse las cuentas en busca de períodos de inactividad o cualquier otro aspecto anormal que permita una redefinición de la necesidad de acceso.

5. Detección de actividades no autorizadas. Además de realizar auditorias o efectuar el seguimiento de los registros de transacciones (pistas), existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas. Algunas de ellas se basan en evitar la dependencia hacia personas determinadas, estableciendo la

obligatoriedad de tomar vacaciones o efectuando rotaciones periódicas a las funciones asignadas a cada una.

6. Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.

7. Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos, ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando "bombas lógicas" o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarias de los sistemas también puede causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente.

Para evitar estas situaciones, es recomendable anular los permisos de acceso a las personas que se desvincularán de la organización, lo antes posible. En caso de despido, el permiso de acceso debería anularse previamente a la notificación de la persona sobre la situación.

ROLES

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los

siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

TRANSACCIONES

También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

LIMITACIONES A LOS SERVICIOS

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

MODALIDAD DE ACCESO

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información.

Esta modalidad puede ser:

- **Lectura:** el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
- **Escritura:** este tipo de acceso permite agregar datos, modificar o borrar información.
- **Ejecución:** este acceso otorga al usuario el privilegio de ejecutar programas.
- **Borrado:** permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.
- Todas las anteriores.

Además, existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

- **Creación:** permite al usuario crear nuevos archivos, registros o campos.
- **Búsqueda:** permite listar los archivos de un directorio determinado.

UBICACIÓN Y HORARIO

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana. De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso.

Se debe mencionar que estos dos tipos de controles siempre deben ir acompañados de alguno de los controles anteriormente mencionados.

III.3.2 CONTROL DE ACCESO INTERNO

PALABRAS CLAVES (PASSWORDS)

Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo. Sin embargo, cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas, encuentra dificultoso recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica.

Se podrá, por años, seguir creando sistemas altamente seguros, pero en última instancia cada uno de ellos se romperá por este eslabón: la elección de passwords débiles.

Sincronización de passwords: consiste en permitir que un usuario acceda con su mismo password a diferentes sistemas interrelacionados y, se actualice en forma automática, en todos ellos, en caso de ser modificado. Podría pensarse que esta es una característica negativa para la seguridad de un sistema, ya que una vez descubierta la clave de un usuario, se podría tener acceso a los múltiples sistemas a los que tiene acceso dicho usuario. Sin embargo, estudios hechos muestran que las personas normalmente suelen manejar un solo password para todos los sitios a los que tengan acceso y, que si se los fuerza a elegir diferentes passwords, tienden a guardarlas escritas para no olvidarlas, lo cual significa un

riesgo aún mayor. Para implementar la sincronización de passwords entre sistemas es necesario que todos ellos tengan un alto nivel de seguridad.

Caducidad y control: este mecanismo controla el momento en que pueden y/o deben cambiar sus passwords los usuarios. Se define el período mínimo que debe pasar para que los usuarios puedan cambiar sus passwords, y un período máximo que puede transcurrir para que éstas caduquen.

ENCRIPTACIÓN

La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso.

LISTAS DE CONTROL DE ACCESOS

Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.

LÍMITES SOBRE LA INTERFASE DE USUARIO

Estos límites son utilizados, generalmente, en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas. Básicamente, pueden ser de tres tipos: menús, vistas sobre la base de datos y

límites físicos sobre la interfase de usuario. Por ejemplo: los cajeros automáticos donde el usuario sólo puede ejecutar ciertas funciones presionando teclas específicas.

ETIQUETAS DE SEGURIDAD

Consiste en designaciones otorgadas a los recursos, por ejemplo un archivo, que pueden utilizarse para varios propósitos, tal como control de accesos, especificación de medidas de protección, etc. Estas etiquetas no son modificables.

III.3.3 CONTROL DE ACCESO EXTERNO

DISPOSITIVOS DE CONTROL DE PUERTOS

Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.

FIREWALLS O PUERTAS DE SEGURIDAD

Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa (por ejemplo Internet). Los firewalls permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización. Este tema será abordado con posterioridad.

ACCESO DE PERSONAL CONTRATADO O CONSULTORES

Debido a que este tipo de personal en general presta servicios temporarios, debe ponerse especial consideración en la política y administración de sus perfiles de acceso.

ACCESOS PÚBLICOS

Para los sistemas de información consultados por el público en general, o los utilizados para distribuir o recibir información computarizada (mediante, por ejemplo, la distribución y recepción de formularios en soporte magnético, o la consulta y recepción de información a través del correo electrónico) deben tenerse en cuenta medidas especiales de seguridad, ya que se incrementa el riesgo y se dificulta su administración.

Debe considerarse para estos casos de sistemas públicos, que un ataque externo o interno puede acarrear un impacto negativo en la imagen de la organización.

ADMINISTRACIÓN

Una vez establecidos los controles de acceso sobre los sistemas y la aplicación, es necesario realizar una eficiente administración de estas medidas de

seguridad lógica, lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

La política de seguridad que se desarrolle respecto a la seguridad lógica, debe guiar a las decisiones referidas hacia la determinación de los controles de accesos y requiere especificar las consideraciones necesarias para el establecimiento de perfiles de usuarios.

La definición de los permisos de acceso requiere determinar el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información, determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados.

Así, los diversos niveles de la información requerirán diferentes medidas y niveles de seguridad.

Para empezar la implementación, es conveniente comenzar definiendo las medidas de seguridad sobre la información más sensible o las aplicaciones más críticas, y avanzar de acuerdo a un orden de prioridad descendiente, establecido alrededor de las aplicaciones.

Una vez clasificados los datos, deberán establecerse las medidas de seguridad para cada uno de los niveles.

Un programa específico para la administración de los usuarios informáticos, desarrollado sobre la base de las consideraciones expuestas, puede constituir un compromiso vacío si no existe una conciencia de la seguridad organizacional por parte de todos los empleados. Esta conciencia de la seguridad puede alcanzarse mediante el ejemplo del personal directivo, en el cumplimiento de las políticas y el

establecimiento de compromisos firmados por el personal, donde se especifique la responsabilidad de cada uno.

Pero además de este compromiso, debe existir una concientización por parte de la administración hacia el personal, en donde se remarque la importancia de la información y las consecuencias posibles de su pérdida o apropiación de la misma por agentes extraños a la organización.

ADMINISTRACIÓN DEL PERSONAL Y USUARIOS
ORGANIZACIÓN DEL PERSONAL

Este proceso lleva generalmente cuatro pasos:

1. **Definición de puestos:** debe contemplarse la máxima separación de funciones posibles y el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas.

2. **Determinación de la sensibilidad del puesto:** para esto es necesario determinar si la función requiere permisos riesgosos que le permitan alterar procesos, perpetrar fraudes o visualizar información confidencial.

3. **Elección de la persona para cada puesto:** requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto. Asimismo, para los puestos definidos como críticos puede requerirse una verificación de los antecedentes personales

4. **Entrenamiento inicial y continuo del empleado:** cuando la persona seleccionada ingresa a la organización, además de sus responsabilidades

individuales para la ejecución de las tares que se asignen, deben comunicárseles las políticas organizacionales, haciendo hincapié en la política de seguridad. El individuo debe conocer las disposiciones organizacionales, su responsabilidad en cuanto a la seguridad informática y lo que se espera de él.

Esta capacitación debe orientarse a incrementar la conciencia de la necesidad de proteger los recursos informáticos y a entrenar a los usuarios en la utilización de los sistemas y equipos para que ellos puedan llevar a cabo sus funciones en forma segura, minimizando la ocurrencia de errores (principal riesgo relativo a la tecnología informática).

Sólo cuando los usuarios están capacitados y tienen una conciencia formada respecto de la seguridad, pueden asumir su responsabilidad individual. Para esto, el ejemplo de la gerencia constituye la base fundamental para que el entrenamiento sea efectivo: el personal debe sentir que la seguridad es un elemento prioritario dentro de la organización.

III.3.4 NIVELES DE SEGURIDAD INFORMÁTICA

El estándar de niveles de seguridad más utilizado internacionalmente es el TCSEC Orange Book, desarrollado en 1983 de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos.

Los niveles describen diferentes tipos de seguridad del Sistema Operativo y se enumeran desde el mínimo grado de seguridad al máximo. Estos niveles han sido la base de desarrollo de estándares europeos (ITSEC/ITSEM) y luego internacionales (ISO/IEC).

Cabe aclarar que cada nivel requiere todos los niveles definidos anteriormente: así el subnivel B2 abarca los subniveles B1, C2, C1 y el D.

NIVEL D

Este nivel contiene sólo una división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad. En sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autentificación con respecto a los usuarios y sus derechos en el acceso a la información. Los sistemas operativos que responden a este nivel son MS–DOS y System 7.0 de Macintosh.

NIVEL C1: PROTECCIÓN DISCRECIONAL

Se requiere identificación de usuarios que permita el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.

Muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este “super usuario”; quien tiene gran responsabilidad en la seguridad del mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que en una organización encontremos dos o tres personas cumpliendo este rol. Esto es un problema, pues no hay forma de distinguir entre los cambios que hizo cada usuario.

A continuación se enumeran los requerimientos mínimos que debe cumplir la clase C1:

- **Acceso de control discrecional:** distinción entre usuarios y recursos. Se podrán definir grupos de usuarios (con los mismos privilegios) y grupos de objetos (archivos, directorios, disco) sobre los cuales podrán actuar usuarios o grupos de ellos.

- **Identificación y Autentificación:** se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por un usuario sin autorización o identificación.

NIVEL C2: PROTECCIÓN DE ACCESO CONTROLADO

Este subnivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos. Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

Requiere que se audite el sistema. Esta auditoría es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios. La auditoría requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores. Permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

NIVEL B1: SEGURIDAD ETIQUETADA

Este subnivel, es el primero de los tres con que cuenta el nivel B. Soporta seguridad multinivel, como la secreta y ultrasecreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio. A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nóminas, ventas, etc.).

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir, que cada usuario tiene sus objetos asociados. También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.

NIVEL B2: PROTECCIÓN ESTRUCTURADA

Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior. La Protección Estructurada es la primera que empieza a referirse al problema de un objeto, a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel inferior. Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios.

El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

NIVEL B3: DOMINIOS DE SEGURIDAD

Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad. Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega, según las políticas de acceso que se hayan definido.

Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y testeos ante posibles violaciones. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura.

Además, cada usuario tiene asignado los lugares y objetos a los que puede acceder.

NIVEL A: PROTECCIÓN VERIFICADA

Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.

Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

OBJETIVOS

E

HIPOTESIS

IV.1 OBJETIVO GENERAL

- Evaluar el nivel de Seguridad que presenta el Sistema de Información en una Empresa de Autoservicio, para determinar su eficacia, seguridad y confiabilidad.

IV.2 OBJETIVOS ESPECIFICOS

- Identificar las Condiciones Físicas donde opera el Sistema
- Verificar los niveles de confiabilidad en la seguridad del Sistema
- Investigar la capacitación y asesoría proporcionada al personal para la operación del Sistema
- Definir el nivel de Seguridad Integral con que cuenta el Sistema
- Investigar las áreas de la empresa que están autorizadas para interactuar con el sistema.

IV.3 HIPOTESIS

- "El Sistema de Seguridad actual y las condiciones de operación del Centro de Trabajo garantizan la Seguridad de las Operaciones Óptimas en la Empresa".

IV.4 JUSTIFICACIÓN

El amplio desarrollo de las nuevas tecnologías informáticas está ofreciendo un nuevo campo de acción a conductas antisociales y delictivas, manifestadas en formas antes imposibles de imaginar.

La Seguridad en los Sistemas de Información, en específico de una Tienda de Autoservicio, se suele manejar con el amarillismo de los medios no especializados, dificultando esto su accionar y colocando en tela de juicio el arduo trabajo de los especialistas. La mayoría del mundo informático y, de todos en general, desconoce la magnitud del problema con el que se enfrenta; generalmente, no se invierte ni el capital humano, ni el económico, necesarios para prevenir, principalmente, el daño y/o pérdida de la información que, en última instancia es el “Conocimiento” con que se cuenta.

Es necesario conocer los recursos disponibles con que cuenta un sistema para protegerlo. Mientras algunas técnicas son evidentes (seguridad física por ejemplo) otras pautas no lo son tanto e incluso algunas pueden ocasionar una sensación de falsa seguridad.

Muchas de las vulnerabilidades que serán estudiadas, son el resultado de implementación incorrecta de tecnologías, otras son consecuencias de la falta de planeamiento de las mismas, pero la mayoría de los agujeros de seguridad son ocasionados por los usuarios de dichos sistemas y es responsabilidad del administrador detectarlos y encontrar la mejor manera de cerrarlos.

Para ello, una buena organización de puestos y distribución de actividades será de gran ayuda; ya que de esta manera estaremos delimitando y

especificando los usuarios del sistema y sus niveles de acceso, lo cual nos permitirá mantener un mejor control del mismo.

IV.5 ALCANCE

El tema principal sobre el cual estará enfocado el trabajo de investigación es **"Seguridad Informática dentro de una Tienda de Autoservicio"**; tomando como punto de referencia "Comercial La Fuente", tienda de la cual obtendremos la información necesaria para poder realizar dicha investigación.

Analizaremos el sistema de información que ahí se maneja, esto con la finalidad de determinar sus niveles de seguridad física y lógica, para ello nos apoyaremos en la realización de una encuesta al personal que interactúa de manera directa con dicho sistema.

Uno de los posibles inconvenientes que se nos presentarán al llevar a cabo la encuesta, puede ser la confiabilidad y veracidad de las respuestas proporcionadas por parte del personal de la tienda de autoservicio. Por ello, incluiré una entrevista al administrador del sistema para constatar la confiabilidad de las respuestas obtenidas en la encuesta.

Finalmente, durante la realización de la entrevista y la aplicación de las encuestas, es posible realizar observaciones sobre las condiciones de operación de la Empresa.

DISEÑO METODOLÓGICO

V.1 PLANEACIÓN DE LA ENTREVISTA

La investigación de campo se llevará a cabo de la siguiente forma: una entrevista con el Administrador del Sistema y se aplicará una encuesta al personal que lo maneja de forma directa.

En la entrevista con el Administrador del Sistema se pretende incluir los siguientes temas:

- Seguridad en el Sistema de Información que se maneja en la Tienda de Autoservicio, tanto física como lógica.
- Mecanismos de Seguridad Implementados para mejorar la Seguridad del Sistema
- Evolución en la Seguridad del Sistema de Información desde su adquisición a la actualidad.

V.2 PLANEACION DE LA ENCUESTA

La encuesta se ha convertido en una herramienta fundamental para el estudio de las relaciones sociales; las organizaciones políticas, económicas y sociales utilizan esta técnica como un instrumento indispensable para conocer el comportamiento de sus grupos de interés y tomar decisiones sobre ellos.

En el desarrollo de la presente investigación, se ha diseñado una encuesta dirigida al área operativa, teniendo un propósito evaluativo de la seguridad física y lógica del sistema. Dicha encuesta tiene las siguientes características:

- Será de carácter descriptiva, para conocer las características en que opera el sistema

- Estará dirigida al administrador y los usuarios del sistema de información
- Será de carácter personal y unitaria
- Será una encuesta de Difusión Pública, debido a que únicamente utilizaré la información con fines académicos

Finalmente, la encuesta consta de 3 secciones:

- La primera: Operación General de la Empresa, donde se pretende detectar la preparación de los empleados que operan el sistema.
- La segunda: Seguridad Física, donde se pretende conocer más acerca del equipo, las instalaciones y las condiciones con las que cuenta la empresa.
- Y la tercera: Seguridad Lógica, donde se pretende conocer de manera general el manejo del sistema.

V.3 MODELO DE ENCUESTA

A continuación se presenta la encuesta aplicada:

La presente encuesta lleva como finalidad evaluar los niveles de seguridad física y lógica con los que cuenta el sistema de información Entec. La información obtenida se utilizará para fines académicos y sus resultados se mantendrán en completa confidencialidad. Le agradecemos de antemano su colaboración.

Lugar y Fecha: _____

Empresa: _____

Puesto: _____

Antigüedad en la Empresa: _____

Tiempo que lleva utilizando el Sistema: _____

OPERACIÓN GENERAL DE LA EMPRESA:

1. Recibiste algún curso de inducción para uso del sistema.

a) Si b) No

2. La duración del curso de inducción fue de:

a) 1 día b) 2 a 4 días c) 5 o más días

3. Para el desempeño de tus funciones, ¿con qué frecuencia te proporcionan capacitación?

a) Más de 6 veces al año b) De 4 a 6 veces al año

c) De 1 a 3 veces al año d) No se nos proporciona capacitación

4. En caso de presentarse algún conflicto con el sistema, ¿Cómo consideras la respuesta a dicha situación por parte del equipo de soporte técnico de la empresa?

a) Excelente b) Aceptable c) Deficiente d) Nula

5. ¿Cómo consideras las condiciones del equipo de cómputo que utilizas para desempeñar tus funciones dentro de la empresa?

a) Excelente b) Aceptable c) Regular d) Deficiente

6. ¿Cómo consideras las condiciones del Sistema que utilizas para desempeñar tus funciones dentro de la empresa?

a) Excelente b) Aceptable c) Regular d) Deficiente

SEGURIDAD FÍSICA:

7. ¿Cómo consideras la distribución de las computadoras en el área de trabajo dentro de tu empresa?

a) Excelente b) Aceptable c) Regular d) Mala

8. ¿Cuál es tu evaluación con respecto a la instalación eléctrica del equipo?

a) Excelente b) Aceptable c) Regular d) Malo

9. La operación del Sistema ha presentado fallas:

a) Nunca b) Pocas veces c) Regularmente d) Constantemente

10. ¿Cuenta el área de cómputo con señalamientos de seguridad y de restricciones para el óptimo desempeño de tus funciones?

a) Si b) No

11. En caso de algún incendio, cuentan con extintores y con los señalamientos sobre la ubicación de los extintores y salidas de emergencia.

a) Si b) No

12. ¿En qué condiciones consideras que se encuentran los extintores de tu empresa?

a) Excelente b) Aceptable c) Deficiente d) Malo

13. ¿Con qué frecuencia realizan la inspección de los extintores en tu empresa?

a) Cada mes b) De 2 a 4 meses c) De 6 meses a 1 año

14. ¿Cuál de las siguientes eventualidades consideras que puedan presentarse en tu área de trabajo?

a) Inundación b) Filtración de Agua
c) Humedad d) Otras: _____

15. ¿Cómo consideras la distribución del cableado del equipo de cómputo que utilizas para llevar a cabo tus actividades?

a) Excelente b) Bueno c) Regular d) Malo

16. ¿Con qué tipo de ventilación cuenta el área en la que desempeñas tus funciones?

a) Aire acondicionado b) Ventilador c) Ambiente natural

17. ¿Cómo consideras la iluminación en el área donde se encuentran los equipos de cómputo?

a) Excelente b) Aceptable c) Deficiente

18. Sabiendo que la temperatura de una oficina con computadoras debe estar comprendida entre 18 y 21 grados centígrados, en tu área de trabajo se tiene una temperatura:

a) Superior al rango b) Dentro del rango c) Inferior al rango

SEGURIDAD LÓGICA

19. ¿Cómo consideras el desempeño del Administrador del Sistema?

a) Excelente b) Bueno c) Regular c) Deficiente

20. Tu ingreso al Sistema lo llevas a cabo mediante:

a) Tarjeta b) Clave Acceso c) Sin Restricción

21. Indica el nivel máximo de acceso que tienes permitido sobre los recursos y la información del sistema:

a) Lectura b) Escritura c) Ejecución d) Borrado e) Creación

22. De acuerdo al puesto que desempeñas, consideras necesario ampliar tu accesibilidad al sistema para el mejor desempeño de tu trabajo.

a) Si b) No ¿Por qué? _____

Escribe alguna sugerencia o comentario sobre algún punto que no se haya tratado en la presente encuesta en relación con la Seguridad en el Sistema.

RESULTADOS, ANÁLISIS Y DISCUSIÓN

VI.1 COMENTARIOS SOBRE LA ENTREVISTA CON EL ADMINISTRADOR DEL SISTEMA:

El Sistema ENTEC Retail, por tener como manejador de base de datos a Adaptive Server Anywhere (ASA), es bastante seguro en la transmisión de datos ya que incluye opciones de cifrado de 128 bits, tanto para comunicaciones como para el archivo de la base de datos.

El cifrado de la comunicación protege la confidencialidad e integridad de los datos en la medida en que viajan entre el dispositivo cliente y el servidor de bases de datos.

ENTEC Retail maneja auditorías de usuarios, ya que registra cada movimiento que un usuario hace en el sistema como:

- Auditorías de intentos fallidos al acceder al sistema (esto es usuario por usuario).
- Auditorías de cancelaciones unitarias y totales de cada comprobante emitido al cliente.
- Auditoría de devoluciones y créditos.
- Auditorías al eliminar, guardar y modificar algún dato (clientes, proveedores, artículos y configuraciones).
- Cambios de precios (persona que los realizó, día y hora), etc.

Además de la seguridad interna, nosotros como usuarios del Sistema Entec Retail hemos implementado diversos mecanismos de seguridad, como son las tarjetas con código de barras para realizar cancelaciones, devoluciones y créditos de artículos en el punto de venta.

Cabe mencionar que el sistema también cuenta con la opción de acceso por medio de huella digital, para incrementar aun más la seguridad.

El sistema ha evolucionado notablemente en cuanto a seguridad se refiere, desde el momento de su adquisición por la empresa hasta la actualidad, prueba de ello es que en un principio cualquier persona podía accesar libremente a él, tuviera o no relación con su área; ahora únicamente el personal relacionado con él tiene acceso por medio de una clave de acceso o de una tarjeta con código de barras. De esta manera el sistema se ha vuelto más seguro y confiable.

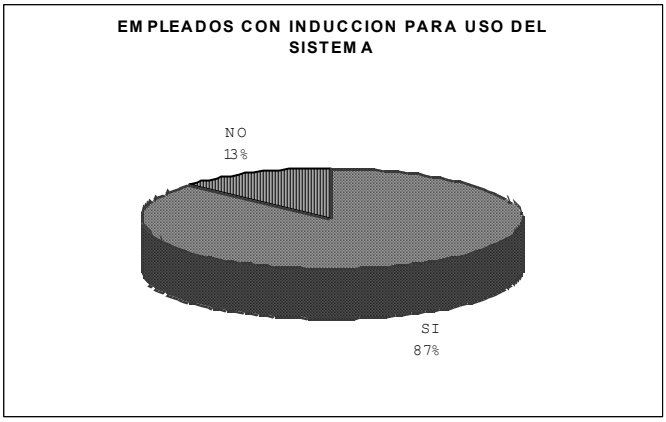
En cuanto a la seguridad de los equipos de cómputo, estos están instalados única y exclusivamente en las áreas que son requeridos, esto con la finalidad de que sólo tengan acceso a ellos el personal autorizado; dicho personal es vigilado constantemente por el administrador del sistema para garantizar la optimización del tiempo de máquina, es decir, que no realicen actividades ajenas a la empresa.

La utilización de guardias de seguridad es imprescindible, ya que permite controlar el acceso de las personas a la empresa. Para ello, el personal debe portar debidamente su credencial de identificación; las personas que son ajenas a la empresa tienen que registrarse antes de ingresar a la misma, y utilizar una credencial con la cual los guardias identifiquen su estancia dentro de la empresa, por ejemplo: personal que está en capacitación, proveedores, visitas, etc.

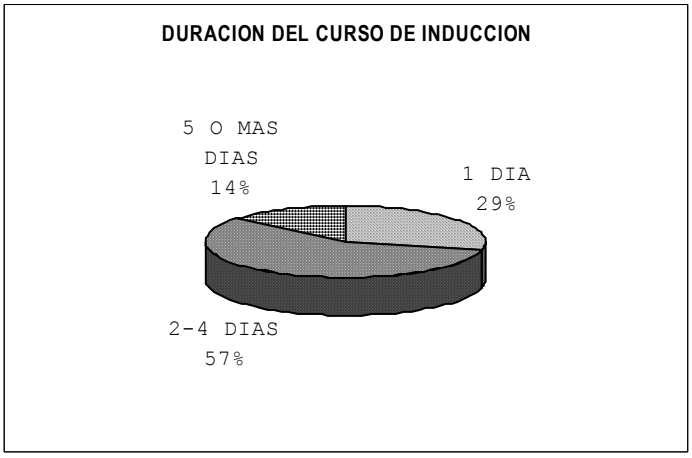
Por último, el administrador afirma: “La seguridad del sistema y de la empresa en sí, es parte fundamental de la misma; por ello se han tomado las medidas necesarias para llevar un control del uso de los equipos, de las actividades realizadas tanto en el sistema como en la empresa en general, así como también del personal. Esto con la finalidad de ofrecer un servicio seguro, confiable y de calidad”.

VI.2 RESULTADOS DE LAS ENCUESTAS APLICADAS AL PERSONAL OPERATIVO:

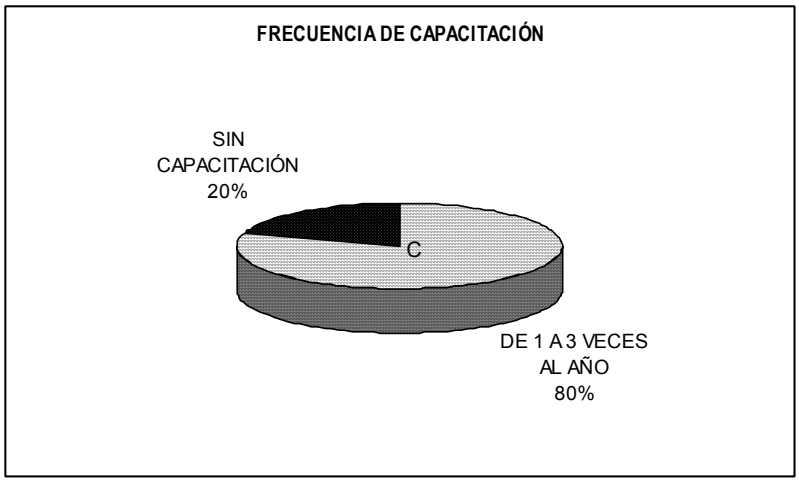
En la siguiente gráfica se muestra el porcentaje del personal que maneja el Sistema ENTEC y que recibió un curso de inducción para el manejo del mismo, al ingresar a la empresa:



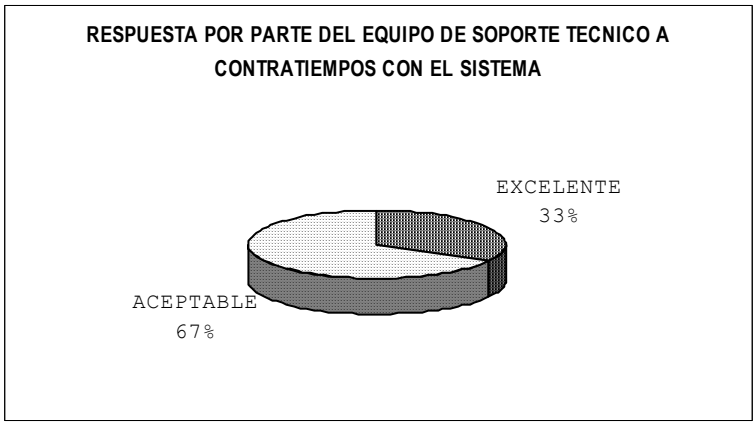
En esta gráfica mostramos el tiempo dedicado al curso de inducción para el manejo del Sistema ENTEC:



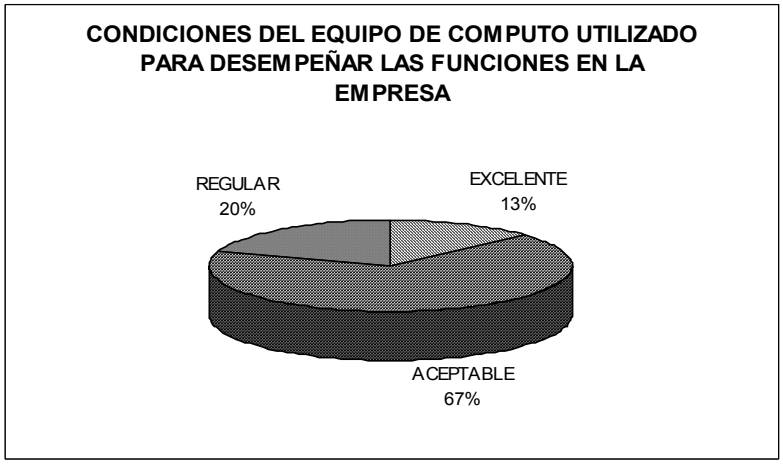
El desempeño de las funciones del personal varía de acuerdo al puesto que ocupan, por ello algunos puestos requieren de una capacitación constante; en esta gráfica se muestra el periodo en que les brindan dicha capacitación:



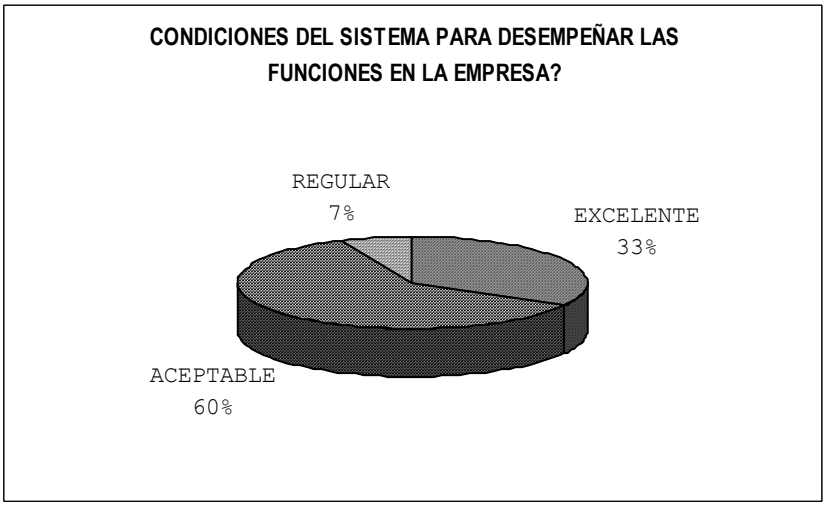
El equipo de soporte técnico de la empresa está completamente capacitado para solucionar cualquier conflicto que pueda presentarse con el sistema. Encuestamos al personal que maneja el sistema para calificar la respuesta que tiene dicho personal ante los conflictos que se han presentado en la empresa y mostramos a continuación los resultados de dicha encuesta:



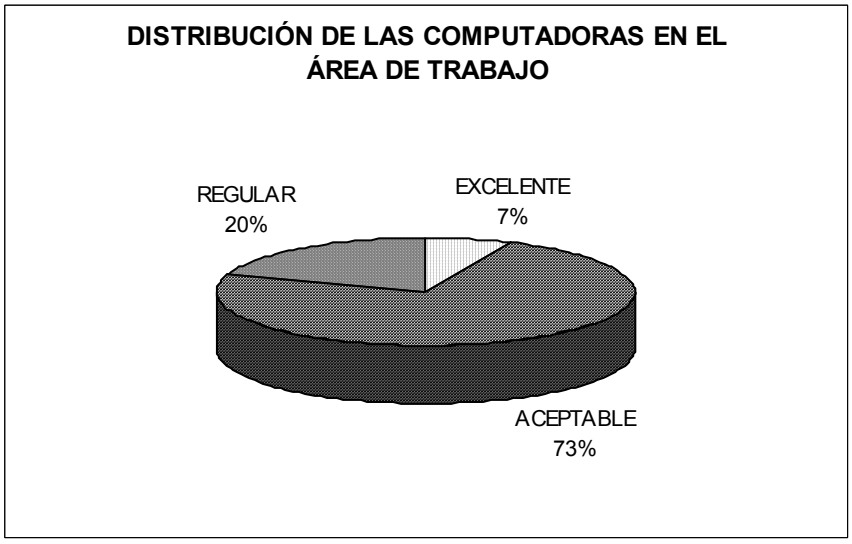
El equipo de cómputo que se debe utilizar en la empresa debe de ser el más completo de acuerdo a las funciones para las que se requiera su uso; la siguiente gráfica muestra las condiciones en que se encuentran los equipos de cómputo en Comercial “La Fuente”:

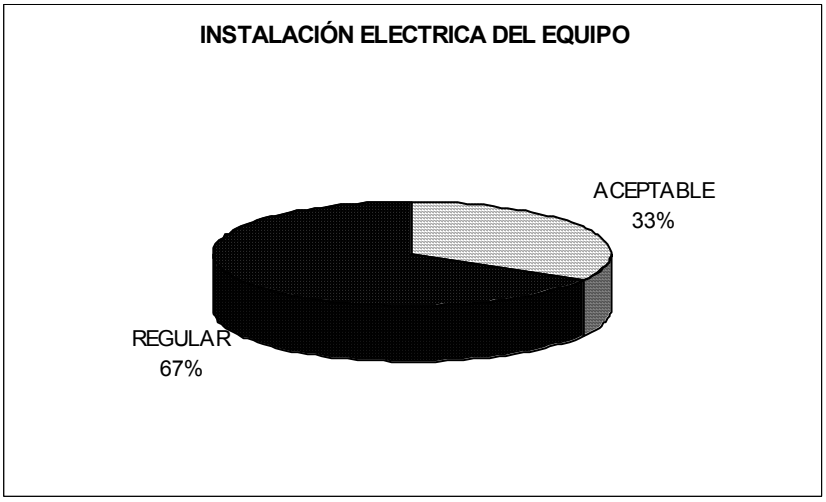


El sistema de información que se debe utilizar en la empresa debe de ser el más completo de acuerdo a las funciones para las que se requiera su uso; la siguiente gráfica muestra las condiciones en que se encuentran el Sistema de Información ENTEC:



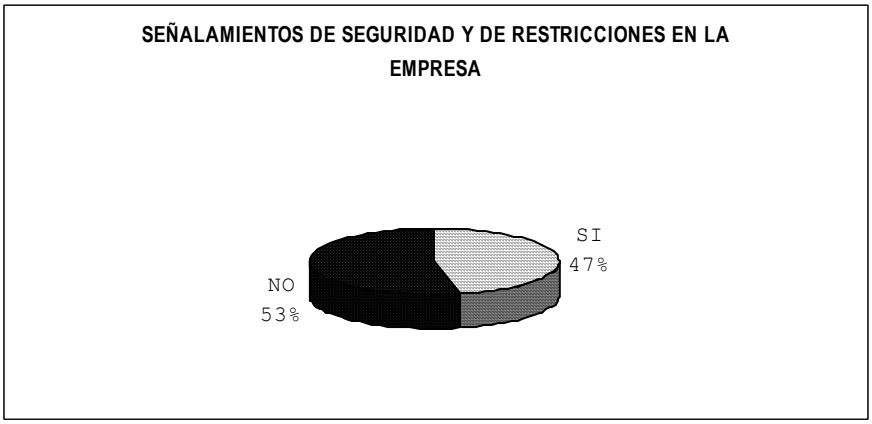
Los equipos de cómputo dentro de cualquier empresa deben estar distribuidos de acuerdo al área de trabajo en la cual se ocupen y las instalaciones de los mismos debe de ser segura y confiable, debido a ello se formularon las siguientes preguntas con las cuales determinaremos como está la actual distribución tanto del equipo como de sus instalaciones eléctricas dentro de la empresa.



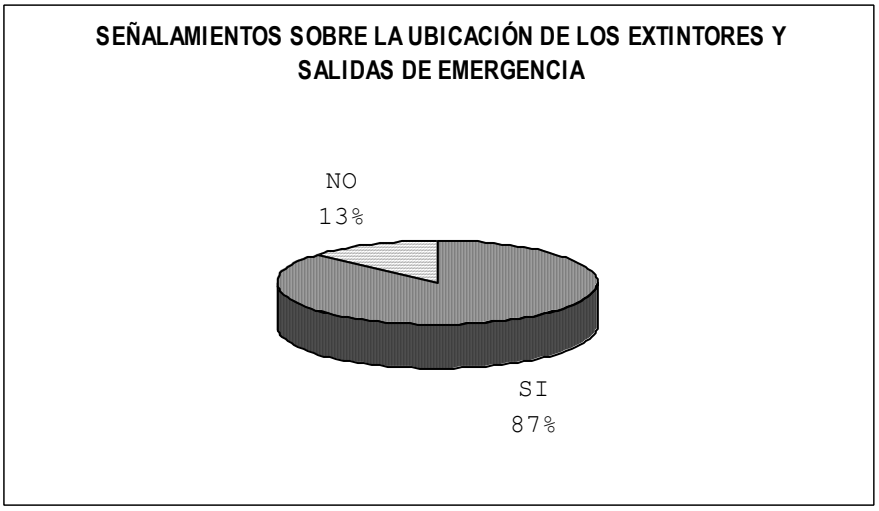


La siguiente gráfica nos muestra que parte del personal ha tenido problemas con el sistema debido a que éste ha presentado fallas; el resultado nos indica la frecuencia con la que se han presentado dichas fallas.

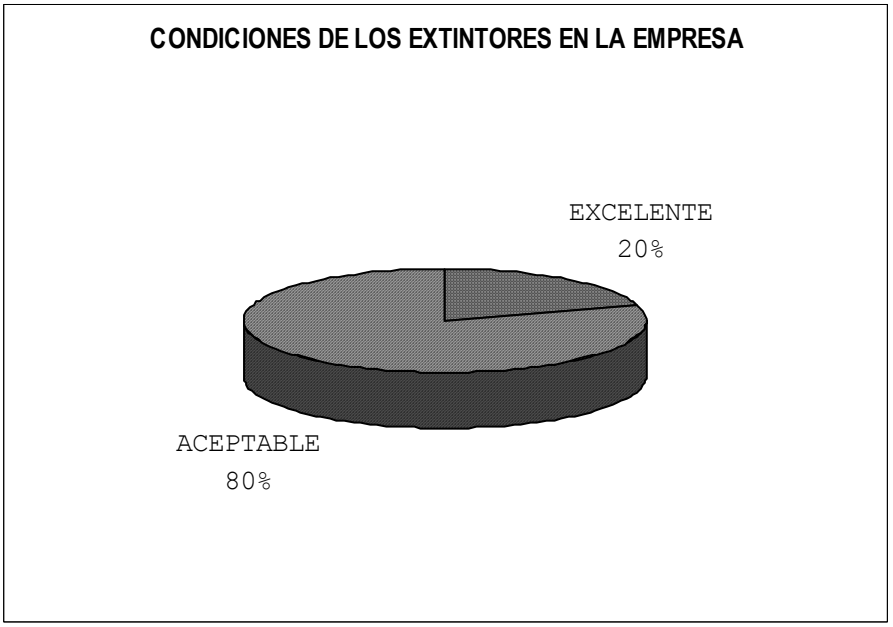
Los señalamientos de seguridad y las restricciones de acceso dentro de una empresa son parte fundamental dentro de la misma; en la siguiente gráfica se muestra qué tan importante es para la empresa estudiada contar con estos señalamientos:



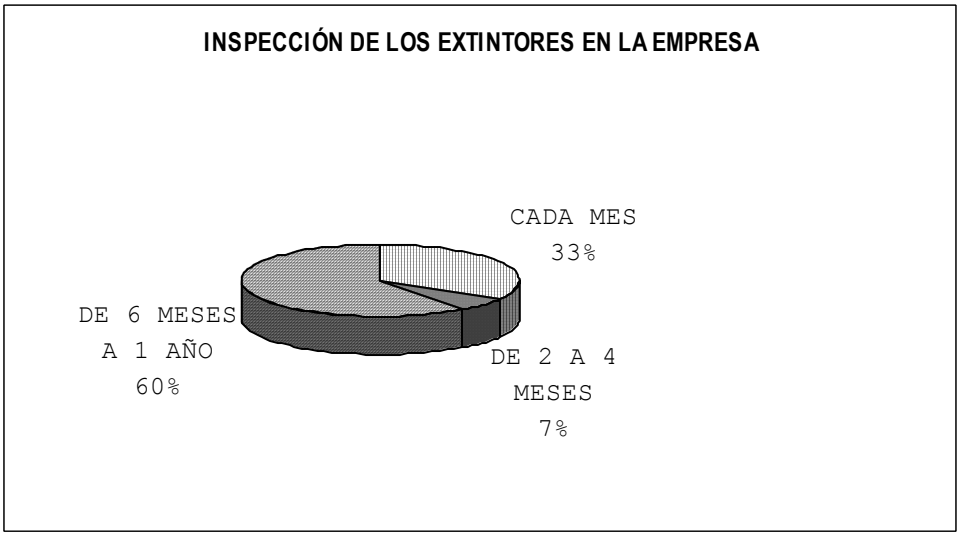
En caso de algún accidente los empleados deben de saber las ubicaciones de extintores y salidas de emergencia, por ello preguntamos a los empleados qué tanto conocen de las ubicaciones de los mismos.



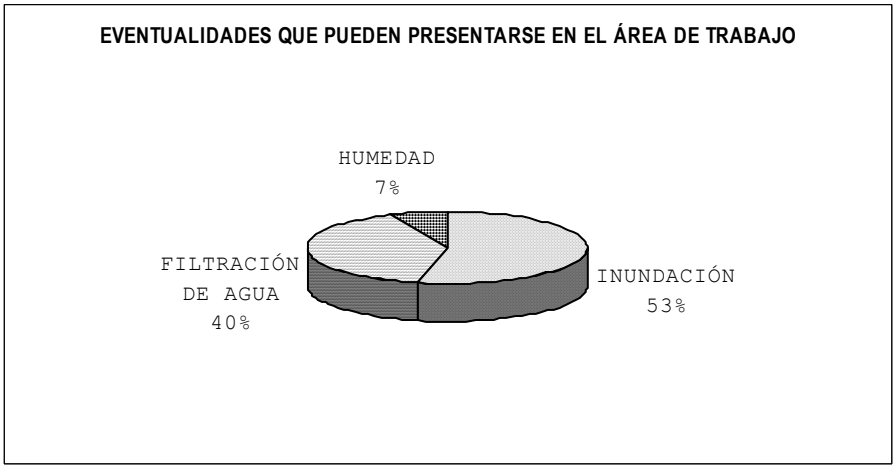
Los extintores deben de estar en óptimas condiciones en caso de utilizarlos, por ello en la siguiente gráfica se muestra en qué condiciones se encuentran.



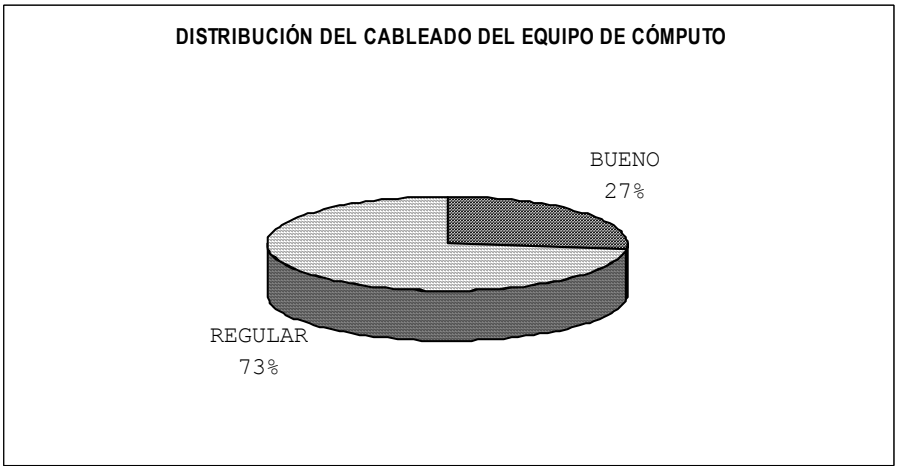
Los extintores deben de recibir una inspección cada determinado periodo para tenerlos en óptimas condiciones en caso de utilizarlos, por ello en la siguiente gráfica se muestra con qué periodicidad reciben dicha inspección.



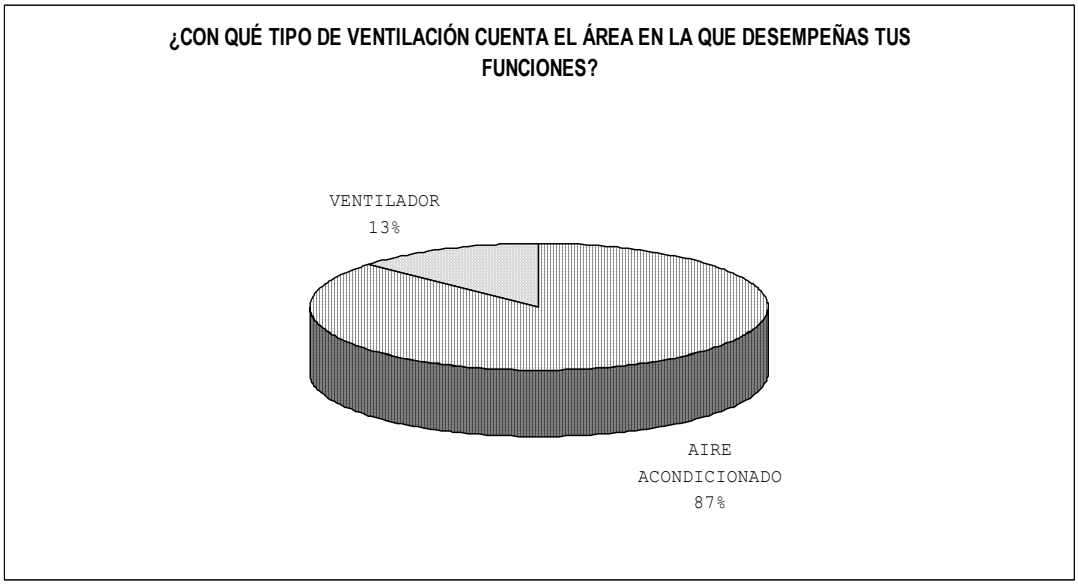
Por la zona en la cual se encuentra localizada la tienda de autoservicio utilizada para nuestro estudio puede presentar diferentes eventualidades, la siguiente gráfica muestra cuales son las que se pueden presentar con mayor probabilidad.



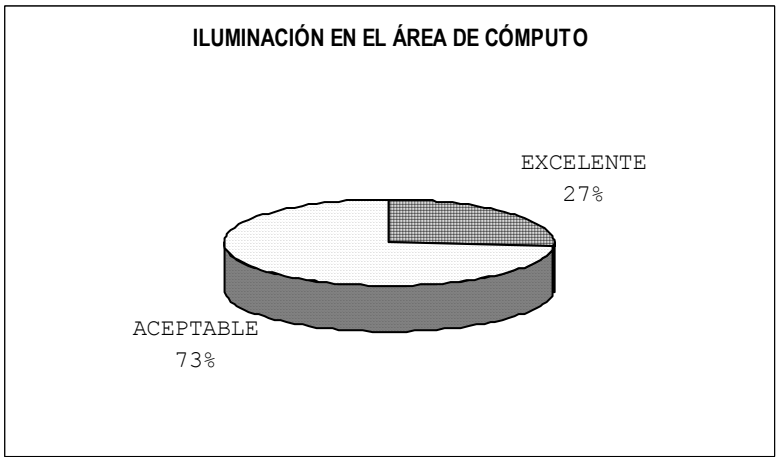
Con la presente gráfica demostraremos qué tan buena es la distribución del cableado de los equipos de cómputo con el que cuenta la empresa.



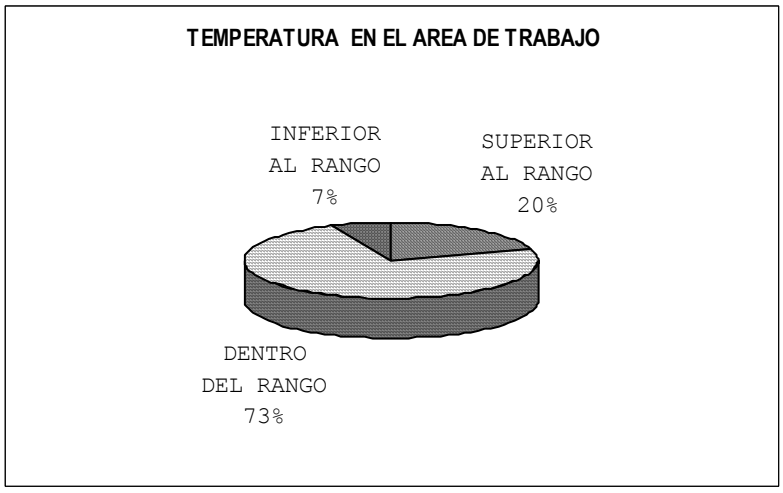
Las áreas en donde se encuentran instalados los equipos de cómputo deben de contar con una excelente ventilación para evitar el sobrecalentamiento de los mismos, en la siguiente gráfica se muestra el tipo de ventilación con que cuenta la empresa.



Las áreas en donde se encuentran instalados los equipos de cómputo deben de contar con una excelente iluminación, en la siguiente gráfica se muestra en qué grado se encuentra la iluminación para dichas áreas.

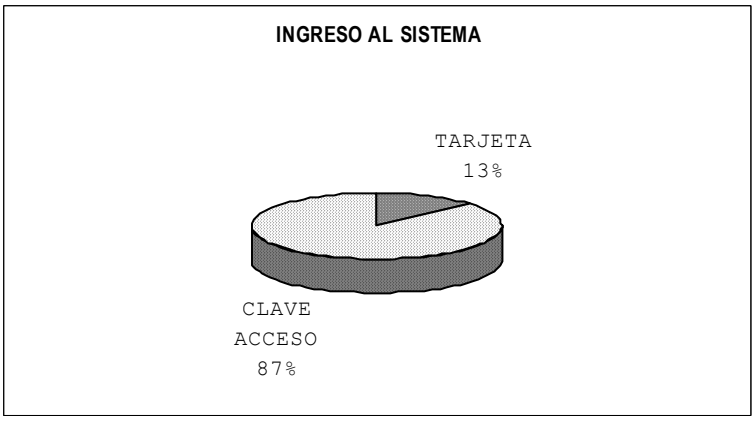


La temperatura en el área donde se encuentran los equipos de cómputo es de suma importancia, por ello, con la presente gráfica se muestra si la temperatura con que cuenta la tienda para esas áreas es o no la adecuada. La temperatura de una oficina debe estar comprendida dentro del rango de 18 a 21 grados centígrados.

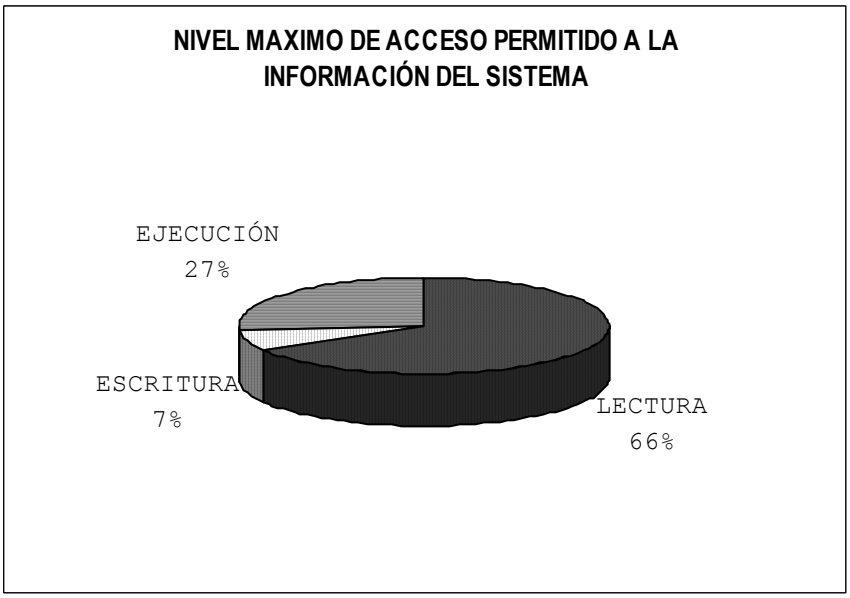


En la siguiente gráfica se califica el desempeño del administrador del sistema, ya que es de suma importancia para la empresa, debido a que es la persona encargada de vigilar el correcto funcionamiento del sistema y en caso de que surja alguna eventualidad debe corregirla a la brevedad para que no afecte a la empresa.

El ingreso al sistema es de dos formas, por tarjeta o por clave, dependiendo de la función del personal varia el acceso al sistema.



Las siguientes gráficas muestran los distintos niveles de acceso con que cuenta el sistema y el porcentaje de empleados que tienen acceso a los mismos; y si ellos consideran necesario ampliar si accesibilidad al sistema o no.



A continuación, haré mención de algunas de las problemáticas detectadas:

- Como pudimos darnos cuenta en el análisis de los resultados de la encuesta, no todo el personal que interactúa con el sistema recibió un curso de inducción; este punto es importante ya que de no utilizar correctamente la información del sistema, se puede generar pérdida de la misma, bloqueo de información o hasta bloqueo del sistema. Por ello es de suma importancia otorgar la capacitación necesaria al personal que trabaja con el Sistema Entec, así como también actualizarlos constantemente.

- Otra de las observaciones hechas durante este trabajo de investigación, es las condiciones en las que se encuentra el equipo de cómputo; ya que al aplicar la encuesta pude observar que un porcentaje de los empleados opinó que el equipo está en condiciones regulares, esto básicamente quiere decir que ha presentado problemas. Lo que hay que hacer aquí es dar un constante mantenimiento a los equipos, esto a su vez ayudará a tener un mejor control sobre el rendimiento de los mismos y en caso de ser necesario, cambiarlos para no originar problemas en la operación de la empresa.

- Al analizar las respuestas otorgadas por parte de los empleados sobre las condiciones del sistema, pude notar que al igual que con el equipo de cómputo, hay quienes han tenido problemas con el sistema. En este caso hay que detectar cuáles son los problemas que presenta el sistema, analizarlos y tratar de solucionarlos a la brevedad.

- La distribución de las computadoras es parte importante de una empresa; al cuestionar sobre este punto, encontré que hay personas

que no están muy de acuerdo con la distribución actual. En este caso, desde mi punto de vista, la distribución que tienen los equipos de cómputo está bien; en la entrada/salida de la tienda de autoservicio se encuentran 4 equipos que son los puntos venta; en el área de paquetería está ubicado otro equipo, el cual es utilizado para dar de alta a los clientes que requerirán factura y para expedirlas; a un costado del almacén se encuentran dos equipos más que están designados al Departamento de Costos y en la planta alta de la empresa se encuentran dos equipos más para el Departamento de Sistemas.

- La instalación eléctrica es otra de las partes de suma importancia, me llamó mucho la atención el porcentaje de empleados que opina que la instalación no es buena. Analizando la instalación, encontré que el mayor problema radica en el área de cajas, debido a que las instalaciones están a nivel del piso y en época de lluvia la tienda se inunda justamente en el área en que se encuentran las cajas, esto puede ocasionar un corto circuito y por ende dañar los equipos.

  En este caso sugiero:

  1. Detectar las áreas donde se inunda la tienda y proceder a repararlas de inmediato.

  2. Cambiar por completo la ubicación de la instalación eléctrica del área afectada con el fin de que no vaya a dañar los equipos en caso de que estos siguieran en contacto con el agua.

- Las fallas en el sistema en un principio eran muy notorias, actualmente se han minimizado considerablemente; uno de los problemas más constantes era en el área de cajas, al no pasar los productos correctamente, esto debido a que la descripción no coincidía, el código estaba duplicado o el precio no era el mismo que estaba en la cenefa. Para disminuir este problema se fue actualizando la base de datos de los artículos, actualmente ya se encuentra más completa en cuanto a la información contenida en ella se refiere.

- Los señalamientos de seguridad, así como los de la ubicación de los extintores dentro de una empresa, son parte fundamental, mas aún cuando hay áreas en las que no se puede accesar sin protección. En este punto, más del 50% de los encuestados opinó que no hay señalamientos en su área de trabajo. Realicé una inspección y me encontré con que si hay señalamientos de seguridad y extintores, pero no se encuentran visibles, de modo que la mayoría de los empleados no se han percatado de su existencia dentro de la empresa.

- Al preguntar acerca de la periodicidad con que se inspeccionan los extintores, encontré que no hay una igualdad en los periodos de inspección en todas las áreas. Por lo que aquí solo puedo sugerir que se determine un solo periodo para realizar la inspección y tener todos los extintores en excelentes condiciones.

- Debido a la ubicación de la tienda de autoservicio estudiada, encontré específicamente 3 eventualidades, las cuales son: Humedad, Filtración de Agua e Inundación, siendo esta última la de mayor problema. Motivo por el cual hay que detectar en donde se origina dicho problema y

solucionarlo a la brevedad ya que puede causar daños severos para la empresa.

CONCLUSIONES

Cuando se diseña un sistema se hace pensando, principalmente, en su Operatividad–Funcionalidad y en muchas ocasiones no se atiende adecuadamente el aspecto de su Seguridad; es necesario establecer un vínculo entre las técnicas adoptadas, conformando un sistema de seguridad y no procedimientos aislados que contribuyan al caos general existente. Esto sólo puede lograrse al integrar la seguridad desde un principio, con el diseño y el desarrollo del sistema.

Algunos métodos realmente novedosos de infiltración ponen en jaque los sistemas de seguridad. Aquí, se prueba la incapacidad de lograr un sistema 100% seguro, pero también es hora de probar que los riesgos, la amenaza y, por ende, los daños pueden ser llevados a su mínima expresión.

Muchas veces basta con restringir accesos a información no utilizada o que no corresponde a los fines planteados. Otras veces la capacitación será la mejor herramienta para disminuir drásticamente los daños y la persona encargada de realizar estas actividades es el Administrador del Sistema.

Existe una gran diferencia entre el Administrador del Sistema y el Intruso; mientras que un intruso penetra en las redes para distintos fines (investigación, daño, robo, etc.) un administrador lo hace para poder mejorar la seguridad en el sistema.

Es posible dividir las tareas de administración de seguridad en tres grandes grupos, los cuales son: la autenticación, la autorización y la auditoria.

En este caso, y como se vino mencionando a lo largo del trabajo, una capacitación constante, la organización de puestos, distribución de actividades y una vigilancia constante de la utilización del sistema, serán nuestras mejores

armas; debido a que sólo las personas involucradas con el sistema tendrán acceso al mismo. De esta manera estaremos minimizando gran parte del riesgo a que la seguridad de éste sea violada.

Por regla general, las políticas son el primer paso que dispone a una organización para entrar en un ambiente de seguridad, puesto que reflejan su "voluntad de hacer algo" que permita detener un posible ataque antes de que éste suceda.

Hay diferentes maneras para proteger a los sistemas de información, algunos de los métodos de protección más comúnmente empleados son: sistemas de detección de intrusos, sistemas orientados a conexión de red, sistema de análisis de vulnerabilidades, sistemas de protección a la integridad de información, sistemas de protección a la privacidad de la información, entre muchos otros.

Cabe mencionar que tuve la oportunidad de operar de manera directa el Sistema desde su implementación, y fue precisamente por esa causa que me surgieron muchas interrogantes referentes al funcionamiento del sistema, por lo que puedo efectuar los siguientes comentarios:

- Las condiciones del sistema en un principio no eran las adecuadas para garantizar la seguridad del mismo; pero, a medida que se fue haciendo el cambio del sistema utilizado anteriormente por la empresa al Sistema Entec, se fueron analizando las herramientas con las que cuenta el sistema y que nos podrían ayudar a hacerlo mas confiable y seguro.

- Algunas de las problemáticas que surgieron, fue el libre acceso que tenían los empleados en general al sistema, esto podría ser causa de problemas fuertes en la operación de la empresa.

- Como un ejemplo, mencionaré lo siguiente: Si un empleado entraba a la base de datos y borraba información de los artículos, ya sea toda la información o parte de ella, estos ya no pasarían por caja o el punto de venta y ya no estarían registrados en el reporte de venta del día; por lo consiguiente, afectaría al inventario de la tienda y el corte de caja final, marcando la cantidad total que resultaría de los productos no registrados como faltante en la entrada del día. Esto, es solo una de las diversas problemáticas que podrían presentarse de no utilizar correctamente la información que guarda el sistema.

En la actualidad, se han implementado claves de acceso al personal que tiene que utilizar el sistema y únicamente al área que le corresponda. De esta manera estamos garantizando que la información que se maneje en el sistema es segura y confiable.

Para esto, se realizó un estudio de puestos, determinando las funciones de cada uno de los empleados, y con ello analizar que tan necesario era la interacción del empleado con el sistema.

Así, las únicas personas que pueden hacer modificaciones en el sistema son: el administrador del sistema y la encargada de costos; esto con la finalidad de evitar que haya intrusos en el mismo.

Como resultado de la presente investigación a las condiciones de operación de “Comercial La Fuente”, podemos afirmar lo siguiente:

- La Seguridad Física del Sistema es buena
- La Seguridad Lógica del Sistema es muy buena

Finalmente, es importante aclarar que para lograr el nivel óptimo en las operaciones del Sistema Entec, únicamente será necesario que exista la voluntad de los directivos en atender las áreas de oportunidad detectadas y comentadas en este documento.

GLOSARIO

Auditoría: Se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este grupo el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

Autenticación: Se refiere a establecer las entidades que pueden tener acceso al universo de recursos de cómputo que cierto medio ambiente puede ofrecer.

Autorización: Es el hecho de que las entidades autorizadas a tener acceso a los recursos de cómputo, tengan acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.

Sistemas de análisis de vulnerabilidades: Analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La “desventaja” de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que buscan acceso no autorizado al sistema.

Sistemas de detección de intrusos: Son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, sobre la base de la información con la que han sido previamente alimentados.

Sistemas de protección a la integridad de información: Sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger.

Sistemas de protección a la privacidad de la información: Son herramientas que utilizan criptografía para asegurar que la información sólo sea

visible para quien tiene autorización. Su aplicación se realiza principalmente en las comunicaciones entre dos entidades.

Sistemas orientados a conexión de red: Monitorizan las conexiones que se intentan establecer en una red o equipo en particular, siendo capaces de efectuar una acción sobre la base de métricas como: origen y destino de la conexión, servicio solicitado, permisos, etc.

BIBLIOGRAFÍA

“Manual del Sistema Entec Retail Punto de Venta”
TEC ELECTRONICA S.A. DE C.V.

“Seguridad Informática”
Caballero Gil, Pino
Alfa Omega
S/Edición
México, 1997

“Piratas Cibernéticos Cyberwars”
Seguridad Informática e Internet
De Marcelo Rodao, Jesús
RAMA
S/Edición
España, 2001

“Informática Presente y Futuro”
Donald H. Sanders
McGraw-Hill
3ª Edición
México, 1990

“Seguridad en Unix y Redes”.
Huerta, Antonio Villalón
Versión 1.2 Digital
Open Publication License v.10 o Later

PÁGINAS VISITADAS:

http://www.kriptopolis.com
Agosto de 2006.

http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
Agosto de 2006.

http://es.wikipedia.org/wiki/Sistema_de_información
Agosto de 2006.

Nota: Por el continuo movimiento de las direcciones de Internet es posible que alguna de las enumeradas no se encuentren disponibles para consulta.