Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela de Contabilidad Superior

EVALUACIÓN DE RIESGOS AL SISTEMA INFORMÁTICO CONTABLE DE LA EMPRESA SAFEGUARD CIA. LTDA.

Trabajo de graduación previo a la obtención del título de

Ingeniero en Contabilidad y Auditoría

Autores: **Cruz Segarra Rodrigo Alexander**

Vidal Beltrán Freddy Rolando

Director: Ing. Jorge Iván Espinoza Idrovo

Cuenca, Ecuador

2008

DEDICATORIA

Cada objetivo cumplido con esfuerzo tiene un propósito, el simple hecho de culminarlo con éxito es un motivo para mirar al cielo y decir gracias Dios por todo lo que me das cada día, por mis padres con su paciencia y comprensión, a mis hermanos, cuñados y a la gran bendición mis sobrinos Doménica y Mathew, a mis amigos y compañeros de toda la vida.

RODRIGO CRUZ S.

DEDICATORIA

Esta monografía la dedico en primer lugar a Dios por permitirme finalizar con éxito esta etapa importante de mi vida, luego a mis padres quienes desde el inicio me apoyaron e inculcaron valores de honestidad y superación personal; finalmente a mi enamorada por toda la comprensión y paciencia durante el transcurso de este trabajo.

FREDDY VIDAL B.

AGRADECIMIENTO

A mi querida Universidad, en donde me formé como profesional en el área de Sistemas y ahora en Contabilidad y Auditoría, a su personal docente, en especial al Ingeniero Jorge Espinoza nuestro director, a mi amigo y compañero Ing. Diego Condo.

RODRIGO CRUZ S.

AGRADECIMIENTO

Gracias a la Universidad del Azuay por todos los conocimientos adquiridos, a todos sus profesores y en especial al Ing. Jorge Espinoza por su apoyo incondicional en el desarrollo de esta monografía.

FREDDY VIDAL B.

Índice de Contenidos

Índice de Ilustraciones y Cuadros

RESUMEN

En la actualidad es de suma importancia para las organizaciones disponer de información veraz, oportuna y que sea una herramienta para la toma de decisiones en las actividades que estas desarrollan; con el avance de la tecnología las organizaciones se ven en la necesidad de realizar evaluaciones de los riesgos a los cuales están sometidos, tomando mayor realce el área informática y en especial a sus sistemas contables, razón por la cual se crean herramientas para evaluar los riesgos al sistema informático contable que es el tema de desarrollo de este trabajo, en donde se aporta con conceptos, ideas y métodos, con el fin de tener un control adecuado ante la presencia de riesgos que de llegar a materializarse, causarían un impacto en las actividades de le empresa.

ABSTRACT

Nowadays it is of great importance for organizations to have access to correct and timely information as a tool for decision-making. With the development of technology, organizations see the need to evaluate all possible risks, especially in the area of informatics and more specifically in accounting systems. Due to this, specific tools for risk evaluation of accounting systems are created, which is the subject developed in this project. Concepts, ideas and methods are presented with the aim of having efficient risk control within the company in the event of real problems arising, which could affect the company's activities.

INTRODUCCION

Una de las prioridades actuales en las organizaciones ante su afán de crecimiento y competitividad, es la necesidad de contar con información veraz y oportuna, es así que al hablar específicamente de una empresa dedicada a la seguridad privada y electrónica, SAFEGUARD CIA. LTDA. maneja información que por su naturaleza es uno de los activos más valiosos que posee, por lo que la empresa se ha vuelto dependiente de sus sistemas y de la tecnología; sin embargo, no se han tomado las medidas necesarias para evaluar y administrar los riesgos informáticos existentes y las posibles amenazas.

Ante tales circunstancias es necesario evaluar los riesgos informáticos que nos permitan determinar cuáles son las falencias que se presentan en la empresa y de esta manera proponer las acciones que se consideren necesarias para controlar las mismas.

El objetivo del presente trabajo consiste en evaluar los riesgos informáticos en SAFEGUARD CIA. LTDA. con el propósito de dar a conocer las falencias latentes y recomendar a los administradores los procedimientos que se deben llevar a cabo para salvaguardar la información que maneja la misma.

CAPITULO I

1. Descripción de la empresa

1.1 Introducción

La aplicación práctica de nuestro trabajo se desarrollará en la empresa SAFEGUARD CIA. LTDA., la misma que se dedica a brindar el servicio de seguridad privada, física y electrónica. En los últimos años ha experimentado un crecimiento acelerado debido al alto índice de criminalidad, razón por la cual no se han tomado las medidas necesarias para evaluar y administrar los riesgos informáticos existentes.

Se hace necesario realizar la evaluación de riesgos informáticos debido a que la información que maneja la empresa, especialmente en el sistema contable y sus diferentes módulos, es de suma importancia tanto para los usuarios internos como para el cliente o usuario externo, convirtiéndose en uno de los activos más valiosos que posee la empresa por su naturaleza. Dentro de dichos módulos podemos destacar por su importancia la siguiente información: contabilidad en general, tesorería, inventarios, facturación, proveedores y clientes.

1.2 Concepción del Negocio

SAFEGUARD CIA. LTDA., es una empresa privada con personería jurídica de derecho privado, constituida el 15 de julio de 1997 en la ciudad de Quito. Actualmente tiene su centro de operaciones en Cuenca y a nivel nacional, cuenta con una gran infraestructura y experiencia en el ramo por más de once años en el mercado, lo que garantiza un servicio óptimo para brindar tranquilidad y seguridad en estos momentos de alto índice delictivo.

Cuenta con personal de vigilancia correctamente uniformado, armado y entrenado física, intelectual y psicológicamente. El personal reclutado en su totalidad son

exmiembros de las Fuerzas Armadas y Policía Nacional, los cuales son seleccionados y contratados bajo estrictas normas, analíticas y rígidamente evaluados por parte de nuestro departamento de personal e investigación.

La compañía cumple con todos los requerimientos que el Reglamento de Constitución y Funcionamiento de Organizaciones de Seguridad Privada lo exige, así como también con los beneficios de ley para la tenencia y uso de Armamento.

Fotografía 1. Personal de vigilancia de SAFEGUARD

FUENTE: SAFEGUARD CIA. LTDA.

1.3 Misión

Su misión es proteger la vida y la propiedad, mediante la confianza que el público deposita en ella.

1.4 Visión

Su visión es llegar a ser una de las mejores compañías de seguridad y vigilancia privada en el Austro y a nivel nacional gracias a su prestigio, cumplimiento y confianza de sus clientes aportando con un servicio de excelente calidad.

1.5 Objetivos

1.5.1 Objetivo General

Brindar el servicio de vigilancia y seguridad privada a la ciudadanía, y en especial al sector industrial, para lo cual garantiza un servicio de calidad y cumple con las leyes vigentes que regulan esta actividad.

1.5.2 Objetivos Específicos

- Brindar seguridad física por medio de personal de vigilancia capacitado con alto índice de ética y moral a Instituciones Públicas y Privadas, así como a personas naturales.
- Realizar estudios de seguridad, conferencias y asesoramiento.
- Complementar el servicio de seguridad física con sistemas electrónicos de alarmas, cámaras de video, monitoreo y mantenimiento de equipos.
- Custodiar vehículos y flotas con la mercadería que transportan.

1.6 FODA

1.6.1 Fortalezas

- La compañía ofrece un servicio de calidad tanto en la seguridad física como electrónica.
- Es una empresa creada con un Decreto Ministerial que autoriza su funcionamiento a nivel nacional.
- Los directivos y el personal de la empresa tienen altos niveles de conocimiento en el área de seguridad.
- La entidad brinda un servicio de seguridad electrónica y física al mismo tiempo a diferencia del resto de empresas que forman parte de la competencia.
- Cuenta con tecnología de punta en cuanto a seguridad física y electrónica.

- La empresa dispone de información oportuna y veraz, la misma que es generada y almacenada en sus sistemas informáticos.

1.6.2 Oportunidades

- Ampliar el servicio a otras ciudades del país.
- Captar un mayor número de clientes.
- Mantener la imagen de la empresa frente a la competencia.
- Aprovechar el alto índice delictivo que existe en el país.

1.6.3 Debilidades

- No existe un análisis de riesgos informáticos dentro de la empresa.
- El personal para prestar estos servicios es muy escaso en la ciudad, por lo tanto se tiene que contratar personal de otros lugares, debido al alto índice de migración.
- No hay estabilidad en el personal de vigilancia.

1.6.4 Amenazas

- Riesgo de pérdida o robo de información contable de la empresa por usuarios internos y externos.
- Pérdida de información por virus, troyanos, spyware, cracking del computador y spam provenientes de la red de Internet.
- Inestabilidad económica y social del país.
- Competencia desleal.
- Reformas al código de trabajo.
- Riesgos para el personal de vigilancia por alto índice delictivo.
- Pagos impuntuales por parte de las empresas contratantes.

1.7 Conclusiones del capítulo

Luego de conocer detalladamente las actividades a las que se dedica la empresa y el entorno en el que gira su actividad económica, se ve la necesidad de realizar la

evaluación de riesgos al sistema informático contable, el mismo que está conformado por diferentes módulos en los cuales reposa información estratégica para la entidad en su calidad de empresa de seguridad, como son contabilidad en general, tesorería, inventarios, facturación, proveedores y clientes.

CAPITULO II

2. Recolección de teoría referencial de la evaluación de riesgos informáticos

2.1 Introducción a la evaluación de riesgos informáticos

En toda organización es importante contar con una herramienta, que garantice la correcta evaluación de los riesgos, a los cuales están sometidos los procesos y actividades que participan en el área informática; y por medio de procedimientos de control se pueda evaluar el desempeño del entorno informático. De aquí que surge la necesidad de conocer de manera general la teoría referente a nuestro estudio, la cual será revisada en el presente capítulo.

2.2 Conceptos técnicos sobre evaluación de riesgos informáticos

A continuación nombraremos los conceptos que hemos considerado básicos para el correcto entendimiento del contenido de nuestro tema de investigación:

2.2.1 Riesgos

El riesgo puede definirse como aquella condición en la que existe una exposición a la adversidad, conformada por una combinación de circunstancias del entorno, donde hay posibilidad de pérdidas.

La seguridad del software y el análisis del peligro son actividades que permiten garantizar la calidad del software que se centra en la identificación y evaluación de peligros potenciales que pueden impactar al software negativamente y provocar que falle el sistema entero.

Al hablar de sistemas informáticos, hacemos referencia específicamente a los siguientes tipos de riesgos:

2.2.1.1 Riesgos de integridad

Hace referencia a aquellos riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas por una organización. Estos riesgos aplican en cada aspecto de un sistema de soporte de procesamiento de negocio y están presentes en múltiples lugares y momentos en todas las partes de las aplicaciones; no obstante estos riesgos se manifiestan en los siguientes componentes de un sistema:

• **Interface del usuario:** Se relacionan con las restricciones, sobre las individualidades de una organización y su autorización de ejecutar funciones negocio/sistema; considera sus necesidades de trabajo y una razonable segregación de obligaciones.

• **Procesamiento:** Los riesgos en esta área generalmente se relacionan con el adecuado balance de los controles detectivos y preventivos que aseguran que el procesamiento de la información ha sido completado.

• **Procesamiento de errores:** Los riesgos en esta área se relacionan con los métodos que aseguren que cualquier entrada o proceso de información de errores sean capturados adecuadamente, corregidos y reprocesados con exactitud completamente.

• **Interface:** Se relacionan con controles preventivos y detectivos que aseguran que la información ha sido procesada y transmitida adecuadamente por las aplicaciones.

• **Administración de cambios:** Los riesgos en esta área son considerados como parte de la infraestructura y el impacto de los cambios en las aplicaciones. Están asociados con las administraciones inadecuadas de procesos de cambios organizaciones que incluyen: Compromisos y entrenamiento de los usuarios a los cambios de los procesos, y la forma de comunicarlos e implementarlos.

• **Información:** Estos riesgos están asociados con la administración inadecuada de controles, incluyen la integridad de la seguridad de la información procesada y la administración efectiva de los sistemas de bases de datos y de estructuras de datos.

2.2.1.2 Riesgos de relación

Los riesgos de relación se refieren al uso oportuno de la información creada por una aplicación. Se relacionan directamente con la información que sirve para la toma de decisiones.

2.2.1.3 Riesgos de acceso

Estos riesgos se enfocan al inapropiado acceso a los sistemas, datos e información, los cuales abarcan: Los de segregación inapropiada de trabajo, los asociados con la integridad de la información de sistemas de bases de datos y los asociados a la confidencialidad de la información.

2.2.1.4 Riesgos de utilidad

Se enfocan en tres diferentes niveles de riesgo:

• Los riesgos pueden ser enfrentados por el direccionamiento de sistemas antes de que los problemas ocurran.
• Técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas.
• Backups y planes de contingencia controlan desastres en el procesamiento de la información.

2.2.1.5 Riesgos de infraestructura

Se presentan en las organizaciones cuando no existe una estructura de información tecnológica efectiva (hardware, software, redes, personas y procesos) para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente.

2.2.1.6 Riesgos de seguridad general

Son aquellos riesgos que se encuentran inherentes a toda actividad en general como lo son:

- Riesgos de choque de eléctrico: Niveles altos de voltaje.
- Riesgos de incendio: Inflamabilidad de materiales.
- Riesgos de niveles inadecuados de energía eléctrica.
- Riesgos de radiaciones: Ondas de ruido, de láser y ultrasónicas.
- Riesgos mecánicos: Inestabilidad de las piezas eléctricas.

2.2.2 Información

Al hablar de información nos referimos como tal a los activos intangibles que posee la empresa, como lo son por ejemplo la información de clientes, la reputación, la privacidad, el nombre de marca y la información contable en general, es por ello que antes de lanzarse ciegamente a implementar medidas de seguridad debemos conocer muy bien qué es lo que van a proteger y contra qué; para ello debemos identificar cuáles son los activos más valiosos, cuál es su valor, el costo de su reposición y si es posible reponerlos.

2.2.3 Evaluación de riesgos

Parte fundamental dentro de un proceso de administración de riesgos, consiste en identificar aquellos existentes en la organización para posteriormente medir el impacto que generarían cada uno de ellos en caso de llegar a materializarse, determinar su probabilidad de ocurrencia y finalmente asignar prioridades a los mismos para su posterior gestión.

Existen varios criterios que pueden ser usados para establecer una prioridad, enfocada en el impacto financiero potencial de las pérdidas, por ejemplo:

• Riesgos críticos: Son aquellas exposiciones a pérdida en las cuales la magnitud alcanza la bancarrota.

• Riesgos importantes: Son exposiciones a pérdidas que no alcanzan la bancarrota, pero requieren una acción de la organización para continuar las operaciones.

• Riesgos no importantes: Aquellas que no causan un gran impacto financiero.

2.2.4 Gestión de riesgos

La función de la gestión de riesgos consiste en identificar el riesgo, analizar cada uno de ellos para determinar la probabilidad de ocurrencia y el daño que causará si en efecto ocurre. Una vez establecida esta información, los riesgos se priorizan según su probabilidad e impacto. A partir de este análisis se produce un plan de diseño e implementación de medidas de tratamiento y finalmente se efectúa un monitoreo y evaluación a dichas medidas.

2.2.5 Amenazas

"Existen múltiples delitos dentro del mundo digital, todos ellos ligados a la información que se aloja en las aplicaciones informáticas o en los sistemas que se transmiten por las redes de comunicaciones. Las amenazas a la información en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un archivo o una región de la memoria principal, a un destino" (ALVAREZ, G., 2004, pág. 7).

Las cuatro categorías generales de ataques son las siguientes:

- **Creación de información:** Consiste en introducir información nueva dentro de un sistema, lo cual atenta contra la seguridad del mismo.
- **Modificación de información:** Se presenta mediante la alteración de información dentro de los sistemas o mientras viaja por redes de comunicaciones, atacando la integridad de los mismos.
- **Intercepción de información:** Los sistemas informáticos albergan a menudo información sensible, que sólo debería ser accedida por un grupo autorizado de

personas. Si alguien ajeno a este grupo accede a dichos datos se estará incurriendo en un ataque contra la confidencialidad de la información.

- **Interrupción de la información:** Los atacantes también pueden alterar la disponibilidad de los datos alojados en los sistemas, o los que viajan por las redes de comunicaciones. Por tanto, la seguridad informática se ocupará de ser la garante de que la información esté disponible para todo aquel que la necesite y durante todo el tiempo que sea necesario.

2.2.6 Vulnerabilidad

Es un punto en el que un recurso es susceptible de ataque. Los sistemas poseen cierto grado de facilidad para ser atacados, lo cual significa que a mayor vulnerabilidad mayor será la probabilidad de que sean atacados con éxito. Esta inseguridad que presentan los sistemas puede ser enfrentada mediante controles preventivos, detectivos, disuasorios, correctivos o recuperativos.

2.2.7 Impacto

Se define como el daño producido a la organización por un posible incidente. Es el resultado de la agresión sobre el activo.
El Impacto puede ser cuantitativo (si representa pérdidas cuantitativas monetarias directas o indirectas); cualitativo con pérdidas orgánicas (por ejemplo, daño de personas) o con pérdidas funcionales.

2.3 Conclusiones del capítulo

En el presente capítulo hemos logrado definir los conceptos fundamentales que forman parte de una evaluación de riesgos informáticos, dentro de los cuales precisamos los diferentes tipos de riesgos existentes, de qué manera amenazan a un sistema informático y el impacto que ocasionaría su materialidad; definimos también el concepto de información como activo a proteger y el proceso de evaluación del riesgos, así como la manera de gestionar los mismos.

CAPITULO III

3. Aplicación práctica de la evaluación de riesgos informáticos al sistema contable de la empresa SAFEGUARD CIA. LTDA.

3.1 Introducción

La tecnología reinante en los últimos tiempos y la necesidad de agilitar el trabajo en las empresas han hecho que las computadoras se conviertan en la principal herramienta, sin embargo por si solas no servirían de mucho, es allí cuando se ve la necesidad de tener software que sea la interface entre el hardware y el usuario con el único propósito de automatizar ciertos procesos que anteriormente se los venía realizando manualmente, los mismos que llevan mucho tiempo y que muchas veces presentan errores que no garantizan la veracidad de la información.

Con el auge informático y por qué no decir tecnológico, las empresas dieron un gran paso y poco a poco fueron dejando de lado sus procesos manuales y empleando herramientas informáticas cada vez más sofisticadas.

Al mismo tiempo que las empresas se tecnificaban en hardware y software, las amenazas eran más letales haciendo que los riegos sean latentes y muchas veces no evaluados y peor aun administrados.

Dentro de todo este proceso SAFEGUARD vio la necesidad de automatizar sus actividades en el área Administrativa y Operativa, al ser esta una empresa dedicada a la seguridad privada por medio de vigilantes y sistemas electrónicos de seguridad, adquirió paquetes informáticos, los mismos que son una herramienta crucial y que están conectados mediante una red LAN (WIFI) y una WAN (ADSL ETAPA), para compartir sus recursos con los usuarios del sistema.

SAFEGUARD dentro del área Administrativa maneja el sistema SOFI y en el área Operativa los sistemas REPORTER y SISSEG.

3.2 Análisis de la estructura del sistema informático de la empresa

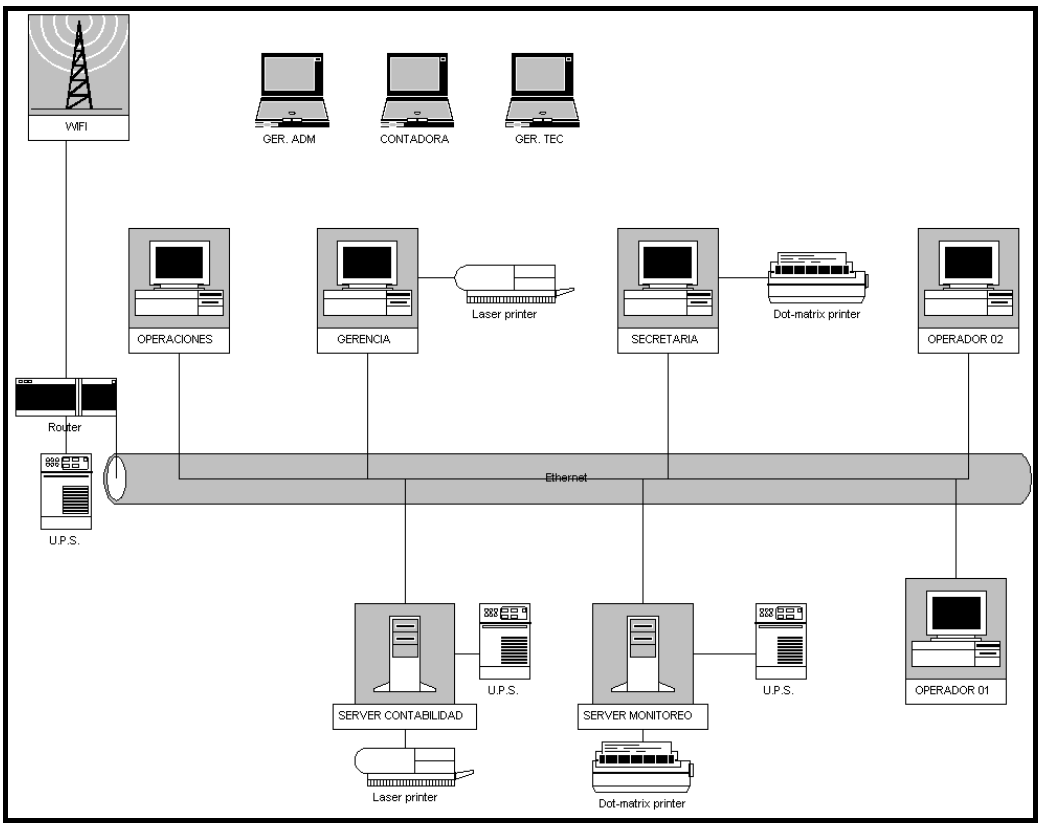
Al hablar de un sistema informático y su estructura, nos vemos en la obligación de hacer un análisis detallado tanto de hardware como de software, con el fin de conocer específicamente cómo está organizado y cómo sus recursos son administrados y compartidos.

3.2.1 Hardware

En la actualidad SAFEGUARD dispone de dos servidores conectados a sus red LAN (Red de área local) de los cuales se desprenden dos grupos de usuarios: por un lado están los usuarios del sistema contable y por el otro está el grupo del sistema de monitoreo, cada grupo con sus respectivos privilegios y restricciones.

El hardware a nivel de la organización se encuentra clasificado según el detalle de la Figura 1.

Figura 1. Hardware general de la empresa SAFEGUARD CIA. LTDA.



FUENTE: SAFEGUARD CIA. LTDA.

La empresa cuenta con una conexión ADSL (conexión de Internet banda ancha), el modem está anclado al router, el cual es un punto de acceso que provee el servicio de internet tanto a los usuarios conectados vía UTP (par trenzado – cable de red) como a los usuarios WIFI (conexión inalámbrica).

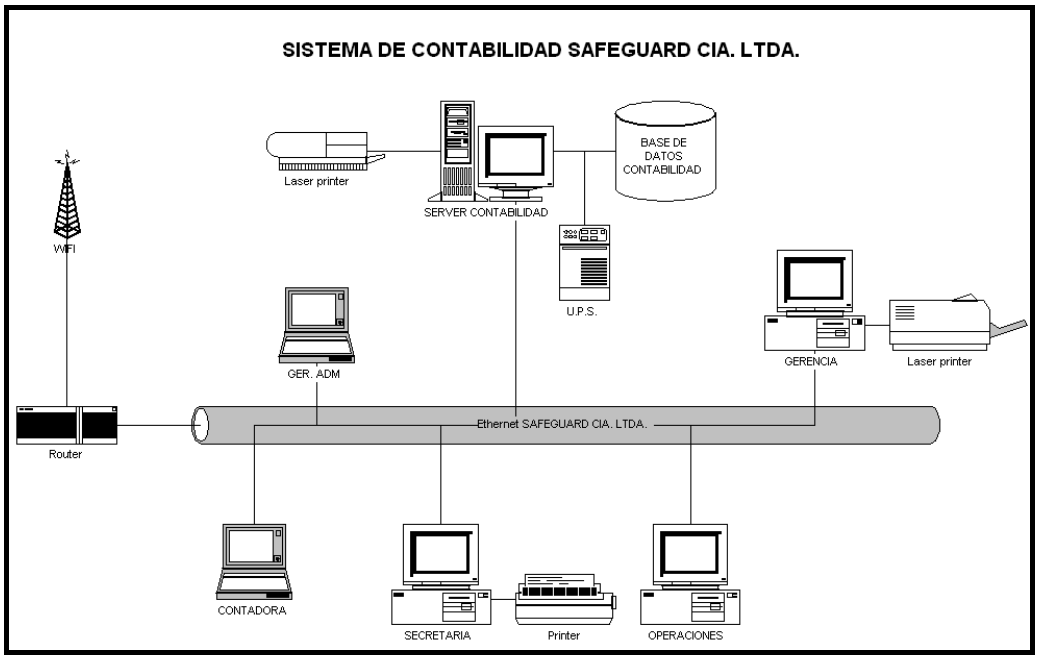
Adicional se dispone de los equipos necesarios para que en caso de una pérdida de energía eléctrica los servidores puedan seguir operando sin problemas (UPS).

3.2.1.1 Hardware de contabilidad

La estructura del hardware que se emplea para el sistema de contabilidad cuenta con un servidor en el que está instalado la base de datos y el sistema informático contable.

Para su funcionamiento este cuenta con tres computadores de escritorio y dos laptops que se encuentran conectados a la red de área local LAN con el propósito de que sus usuarios puedan acceder de forma remota ya sea vía UTP o WIFI, adicional se puede destacar que el servidor de contabilidad cuenta con su respectivo UPS. La figura 2 muestra cada uno de los componentes que conforman el hardware de monitoreo,

Figura 2. Hardware de contabilidad de la empresa SAFEGUARD CIA. LTDA.

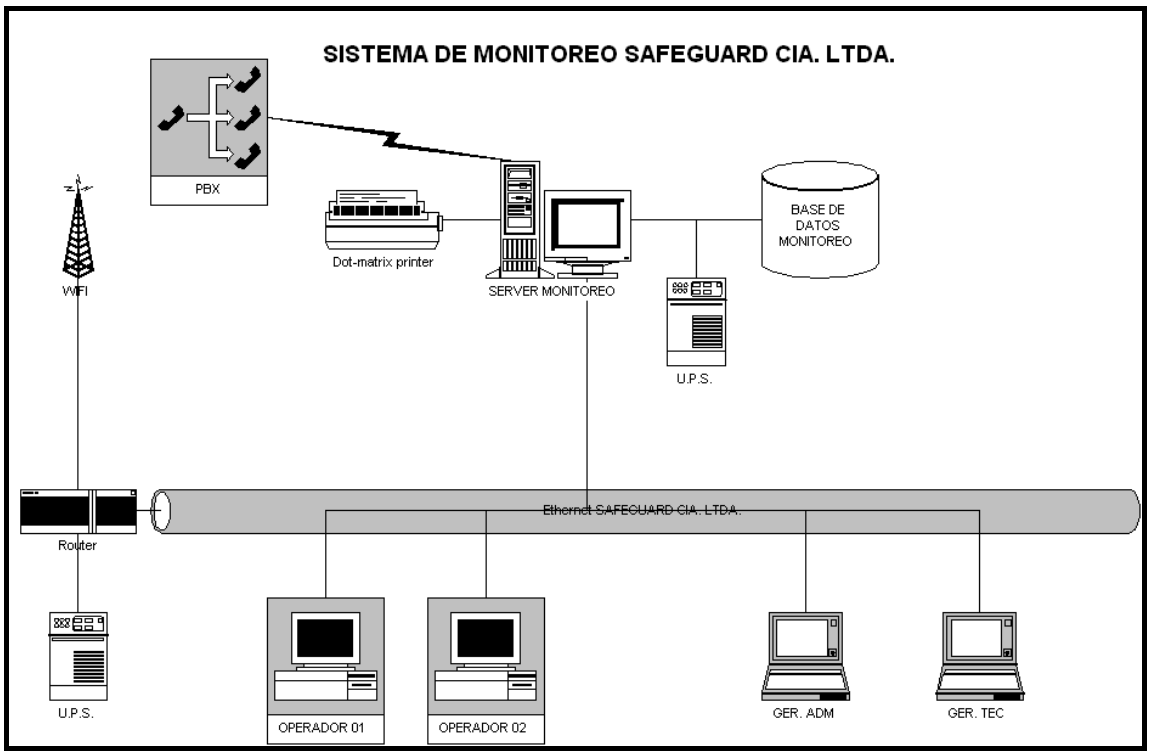


FUENTE: SAFEGUARD CIA. LTDA.

3.2.1.2 Hardware de monitoreo

Al igual que el grupo de usuarios del sistema de contabilidad, en la empresa existe un departamento tecnológico de seguridad, el mismo que funciona las 24 horas en turnos rotativos; los técnicos y monitoristas están pendientes de todos los eventos que se reciban en las consolas de monitoreo, pero esto solo aplica al área de seguridad electrónica. Este grupo de usuarios solo puede acceder al servidor de monitoreo, pero de igual manera tienen acceso a la internet, ya que se encuentran conectados vía UTP, cuentan con las mismas seguridades de acuerdo a su perfil de usuario así como un UPS para el servidor. La figura 3 muestra cada uno de los componentes que conforman el hardware de monitoreo,

Figura 3. Hardware de monitoreo de la empresa SAFEGUARD CIA. LTDA.



FUENTE: SAFEGUARD CIA. LTDA.

Si bien hemos analizado la estructura de hardware a nivel de toda le empresa, cabe señalar que la evaluación de riesgos informáticos será aplicada específicamente al hardware de contabilidad ya que es nuestro tema de estudio.

3.2.2 Software

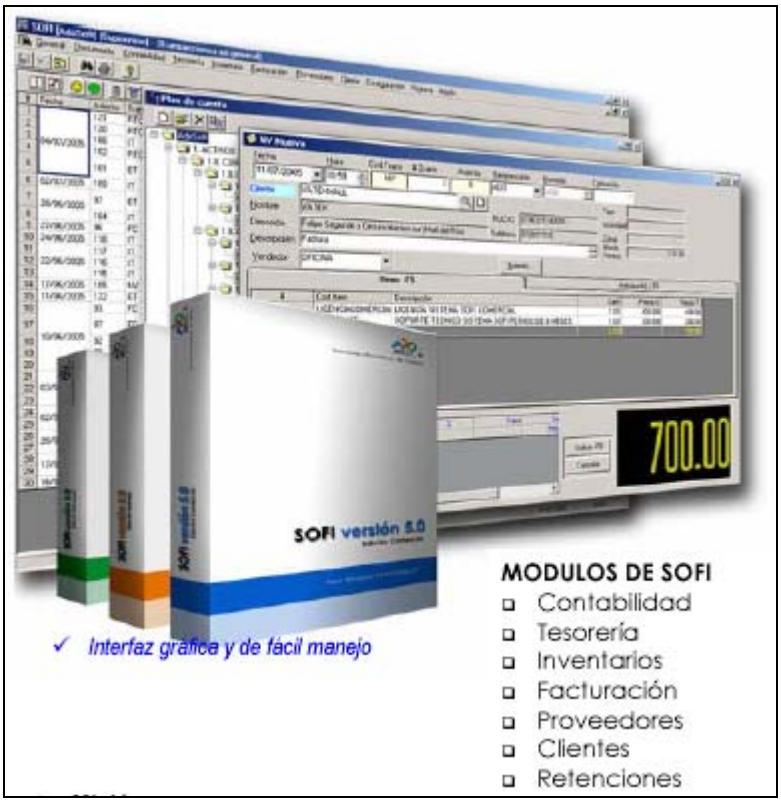
Para el correcto funcionamiento del hardware es necesario disponer del software, el mismo que sirve de interface entre el ordenador y el usuario; de la misma manera si bien nuestro tema de estudio central es el sistema informático contable, no podemos analizarlo de manera aislada ya que este depende del sistema operativo y a su vez se interrelaciona con herramientas informáticas.

Por lo anteriormente expuesto se hace necesario dar una descripción general de cada sistema de software con los que cuenta la empresa para conocimiento y posterior identificación de riesgos.

3.2.2.1 Sistema contable

La empresa utiliza para llevar a cabo su contabilidad el sistema de información automatizado denominado SOFI, siendo una herramienta para el conocimiento, administración, dirección y la toma de decisiones dentro de la empresa.

Figura 4. Sistema SOFI utilizado en SAFEGUARD



Este sistema está desarrollado en Visual Basic 6.0 como lenguaje de programación y su base de datos en SQL Server 7.0 y cuenta con los siguientes módulos integrados:

- Contabilidad
- Tesorería
- Inventarios
- Facturación
- Proveedores
- Clientes
- Retenciones

El sistema lleva un control de documentos, entre los que se encuentran:

- Egresos Bancario
- Ingresos Bancarios
- Cheques
- Ingresos de Materias primas
- Egresos de Materias primas
- Cheques
- Facturas

3.2.2.1.1 Módulo de contabilidad

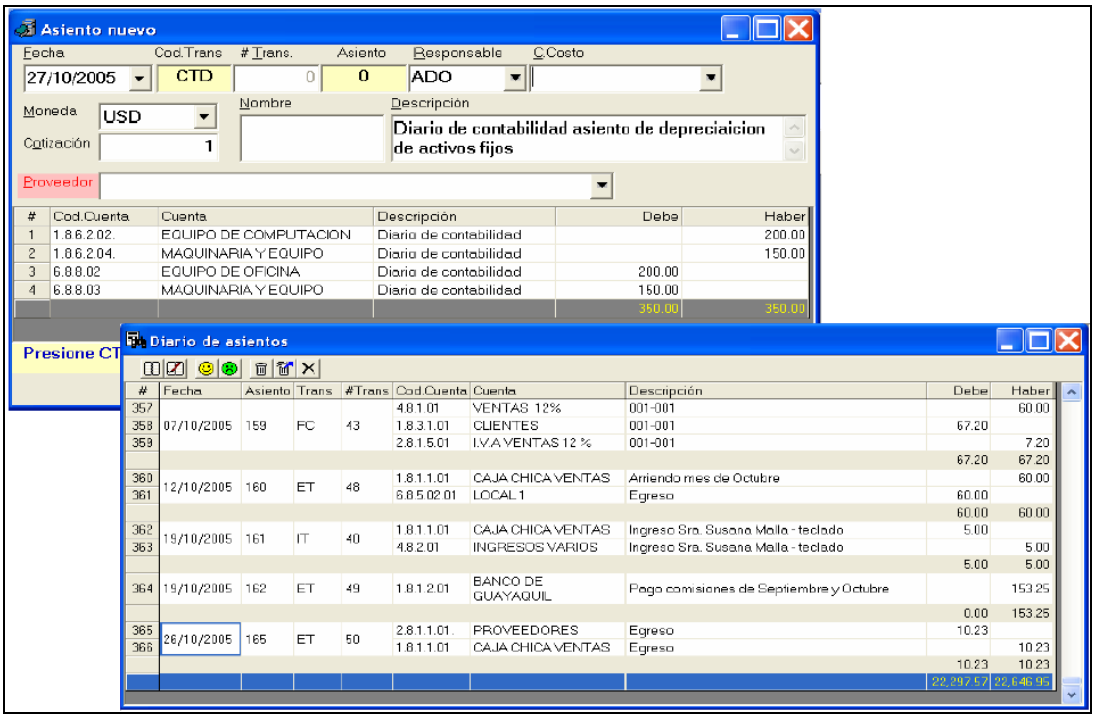
En este módulo se registran individualmente o por lotes cada movimiento o transacción realizada desde cualquier otro módulo, ofreciendo las siguientes cualidades:

- Contabilidad en línea en el momento de cada transacción ya sea desde inventarios, bancos, facturación, u otros.
- Generación de asientos automáticos desde cada uno de los módulos.
- Ingreso de asientos de ajuste, corrección, depreciación, etc.
- Registro del usuario, fecha y hora al momento de ingresar a un asiento contable.

Adicional se puede generar los reportes de:

- Diario
- Libros Mayores
- Balance de Comprobación
- Estado de Pérdidas y Ganancias
- Balance General
- Balance por Mes

Figura 5: Módulo de contabilidad



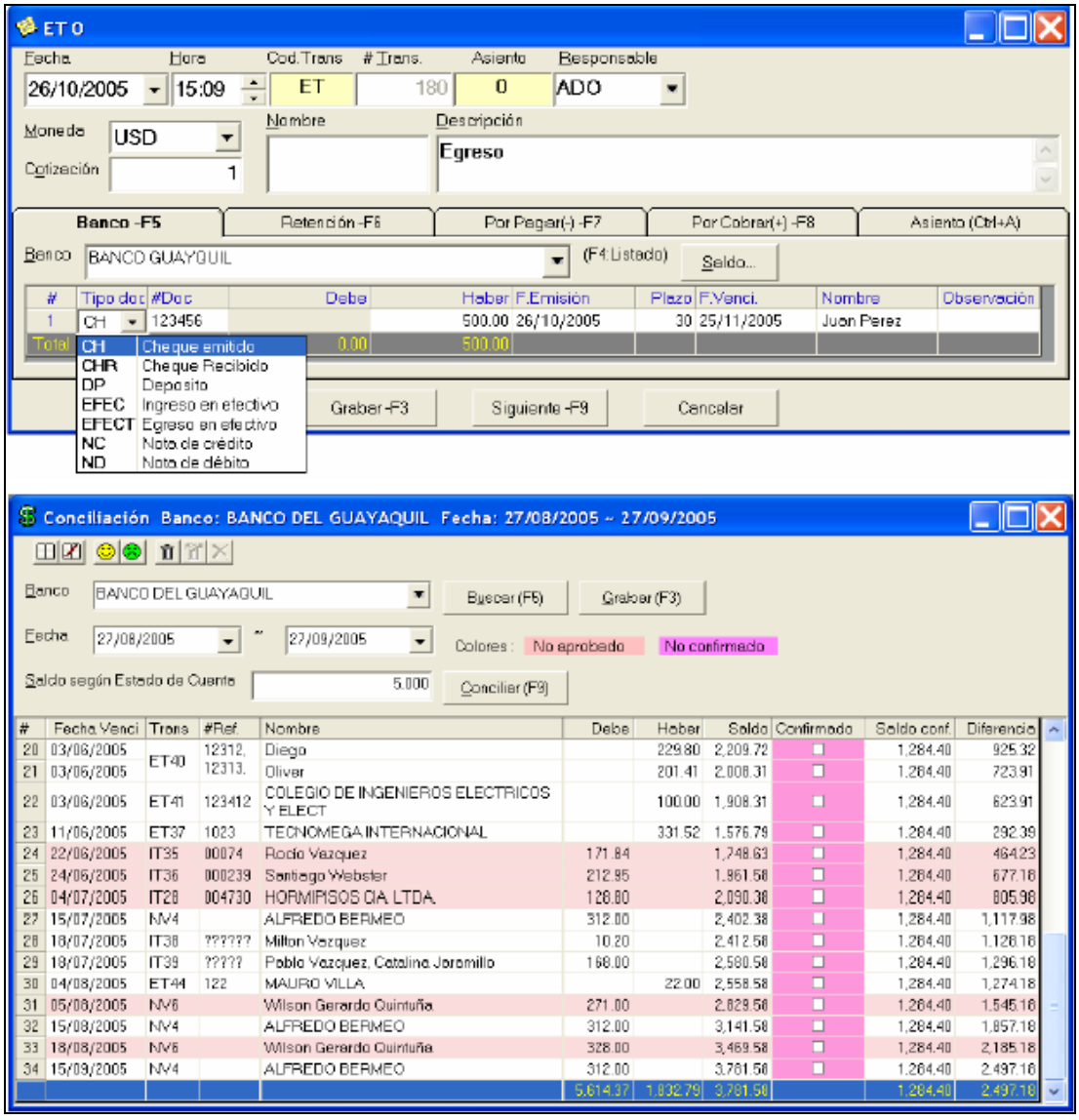
3.2.2.1.2 Módulo de tesorería (bancos)

Los movimientos monetarios de la empresa se operan mediante:

- Manejo de cuentas bancarias, tarjetas de crédito.
- Emisión de ingresos y egresos de bancos.
- Actualización de saldos.
- Control de cheques post - fechados emitidos.
- Control de cheques post - fechados recibidos
- Ingresos y Egresos de notas de débito y notas de crédito bancarios.

- Conciliaciones bancarias.

Figura 6. Módulo de tesorería

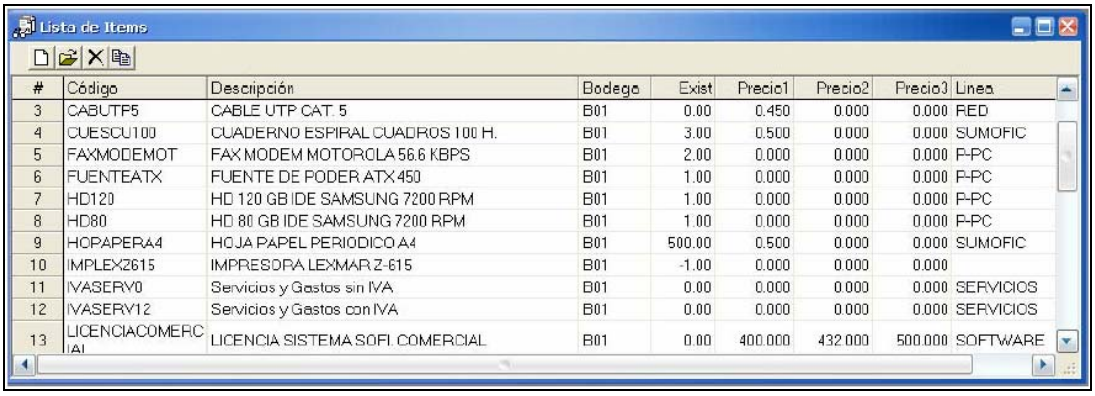


3.2.2.1.3 Módulo de inventarios (stock)

El control de inventarios debe ser cuidadosamente organizado, registrado y controlado debido a la importancia que reviste dentro de cualquier empresa.

En este módulo se actualiza el stock y la disponibilidad en línea relacionando cada ítem con una cuenta contable.

Figura 7. Módulo de inventarios



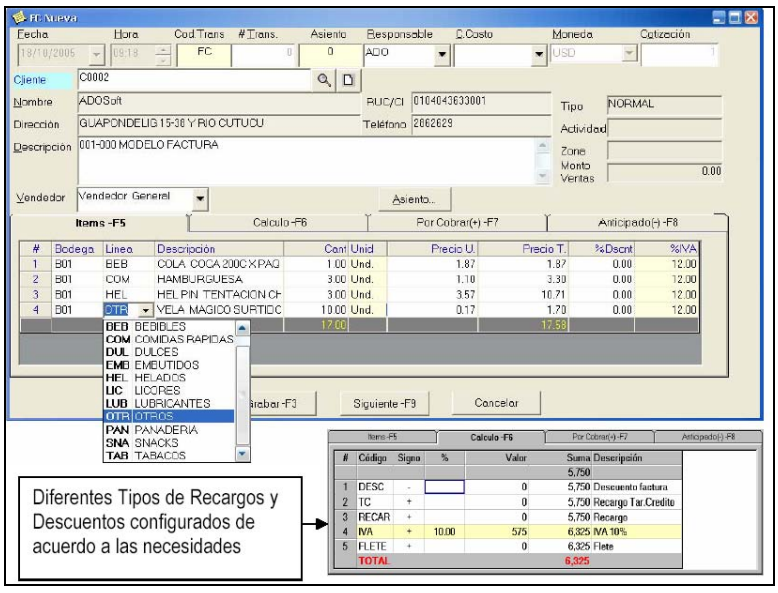
#	Código	Descripción	Bodega	Exist	Precio1	Precio2	Precio3	Linea
3	CABUTP5	CABLE UTP CAT. 5	B01	0.00	0.450	0.000	0.000	RED
4	CUESCU100	CUADERNO ESPIRAL CUADROS 100 H.	B01	3.00	0.500	0.000	0.000	SUMOFIC
5	FAXMODEMOT	FAX MODEM MOTOROLA 56.6 KBPS	B01	2.00	0.000	0.000	0.000	P-PC
6	FUENTEATX	FUENTE DE PODER ATX 450	B01	1.00	0.000	0.000	0.000	P-PC
7	HD120	HD 120 GB IDE SAMSUNG 7200 RPM	B01	1.00	0.000	0.000	0.000	P-PC
8	HD80	HD 80 GB IDE SAMSUNG 7200 RPM	B01	1.00	0.000	0.000	0.000	P-PC
9	HOPAPERA4	HOJA PAPEL PERIODICO A4	B01	500.00	0.500	0.000	0.000	SUMOFIC
10	IMPLEXZ615	IMPRESORA LEXMAR Z-615	B01	-1.00	0.000	0.000	0.000	
11	IVASERV0	Servicios y Gastos sin IVA	B01	0.00	0.000	0.000	0.000	SERVICIOS
12	IVASERV12	Servicios y Gastos con IVA	B01	0.00	0.000	0.000	0.000	SERVICIOS
13	LICENCIACOMERCIAL	LICENCIA SISTEMA SOFI. COMERCIAL	B01	0.00	400.000	432.000	500.000	SOFTWARE

3.2.2.1.4 Módulo de facturación

En lo que respecta al proceso de facturación, se puede referir las siguientes características:

- Acceso independiente por usuarios pre definidos.
- Tiempo de respuesta inmediata en ventas al momento de buscar o digitar un ítem.
- Actualización del inventario en línea.
- Actualización de estadísticas del ítem por ventas realizadas.
- Consultas de disponibilidad y precios, devoluciones.
- Estadísticas y análisis de movimientos de producto.

Figura 8. Módulo de facturación



3.2.2.1.5 Módulo de proveedores (cuentas por pagar)

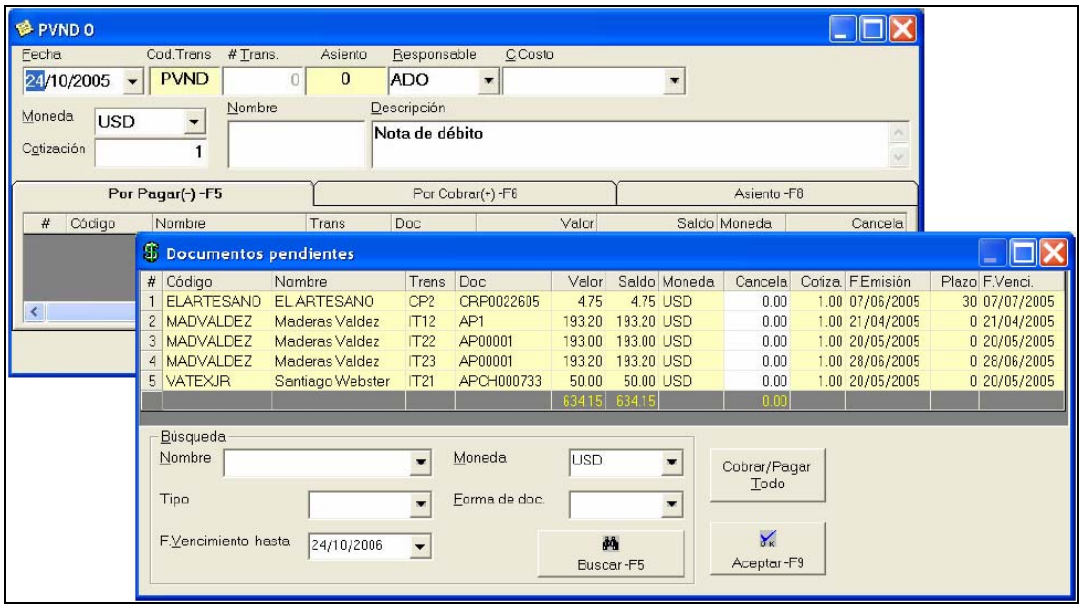
En el módulo en mención se registran todos los datos necesarios respecto a las cuentas de proveedores.

Cuando se realiza una compra el sistema carga automáticamente a la cuenta de cada proveedor, llevando el control de cada pago que se realiza.

Los reportes que genera este sistema son los siguientes:

- Cuentas por pagar a 30 días, a 60 días o a 90 días, etc.
- Saldos de cuentas por cada proveedor.
- Estados de cuenta por proveedor.
- Reportes de pagos.
- Reportes de descuentos.
- Reportes de compras totales o por proveedor.
- Reportes de compras diarios, mensuales, anuales.

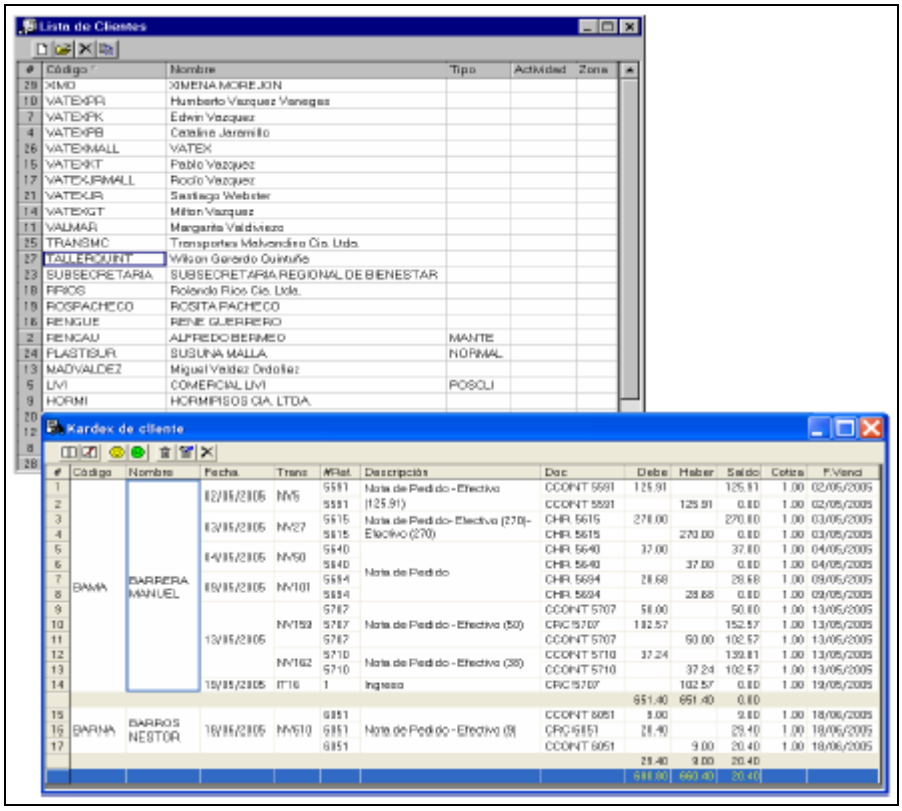
Figura 9. Módulo de proveedores



3.2.2.1.6 Módulo de clientes (cuentas por cobrar)

En este módulo se ingresa, modifica o actualiza la información de cada cliente en la base de datos, se lleva el control de cobros de facturas, letras y demás documentos.

Figura 10. Módulo de clientes



3.2.2.1.7 Módulo de flujo de caja

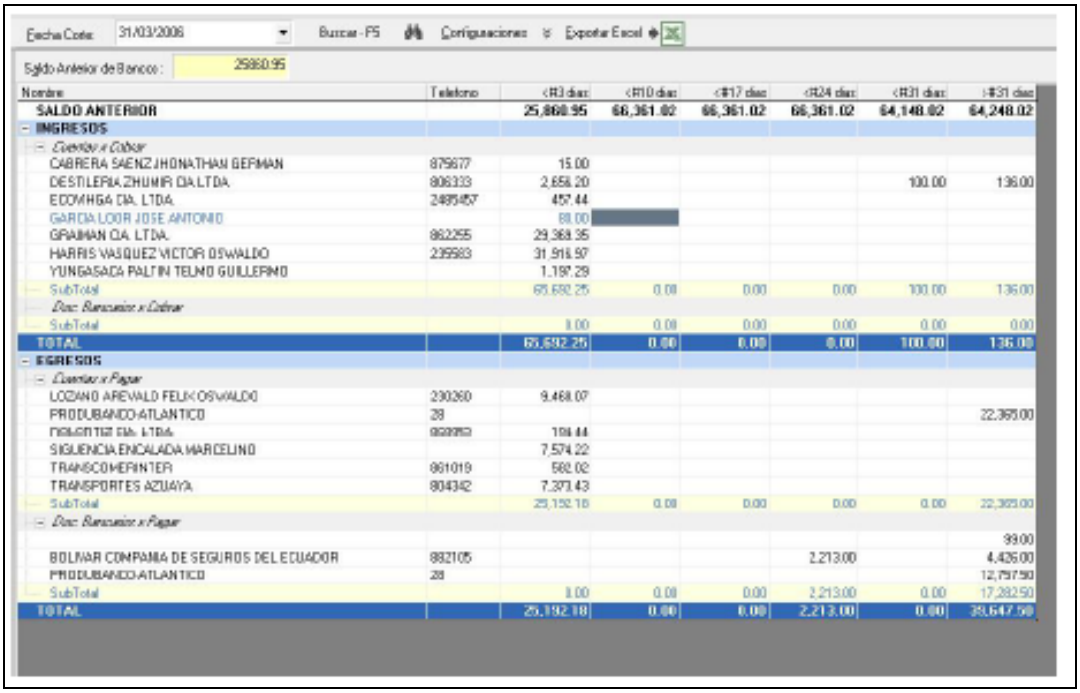
El flujo de caja es una herramienta que permite hacer proyecciones para los pagos, tomando la información de bancos más las cuentas por cobrar, se puede planificar las cuentas por pagar.

El flujo consta de dos partes:

a) Ingresos: son las cuentas por cobrar y cheques posfechados recibidos.
b) Egresos: son las cuentas por pagar y los cheques posfechados emitidos.

Toda está esta información se agrupa por los períodos de vencimientos.

Figura 11. Módulo de flujo de caja



3.2.2.2 Sistema operativo

Los sistemas informáticos que utiliza la empresa trabajan en su totalidad sobre la plataforma Microsoft con su versión de Windows XP Professional con Service Pack 2 con las últimas actualizaciones, el mismo que se encuentra licenciado.

El sistema operativo viene a ser un programa general (que engloba a un conjunto de subprogramas) que nos permite intercomunicarnos directamente con los dispositivos internos y físicos (hardware). Con lo que el sistema operativo en principio trabaja en última instancia con el conocido código binario (0s y 1s).

La existencia de un sistema operativo que brinde todas las garantías necesarias, es de crucial importancia ya que sobre este se instalará cada uno de los sistemas o paquetes informáticos que la empresa requiere para su funcionamiento y operación.

Figura 12. Detalle del sistema operativo que posee SAFEGUARD

3.2.2.3 Herramientas informáticas

Dentro de las herramientas que dispone SAFEGUARD se pueden mencionar las más importantes utilizadas por el área de contabilidad.

3.2.2.3.1 Microsoft Office

La empresa cuenta con el paquete de Microsoft Office y sus respectivos programas como lo son:

- Word
- Excel
- PowerPoint
- Access
- One Note
- Outlook
- Publisher
- InfoPath
- Groove

Figura 13. Herramienta de Microsoft Office utilizadas por SAFEGUARD

El propósito de este paquete informático es permitir que el usuario tenga información fácil, generada por él mismo, que se encuentre disponible cuando el usuario lo requiera y que sea portable.

3.2.2.3.2 Navegador web y correo electrónico

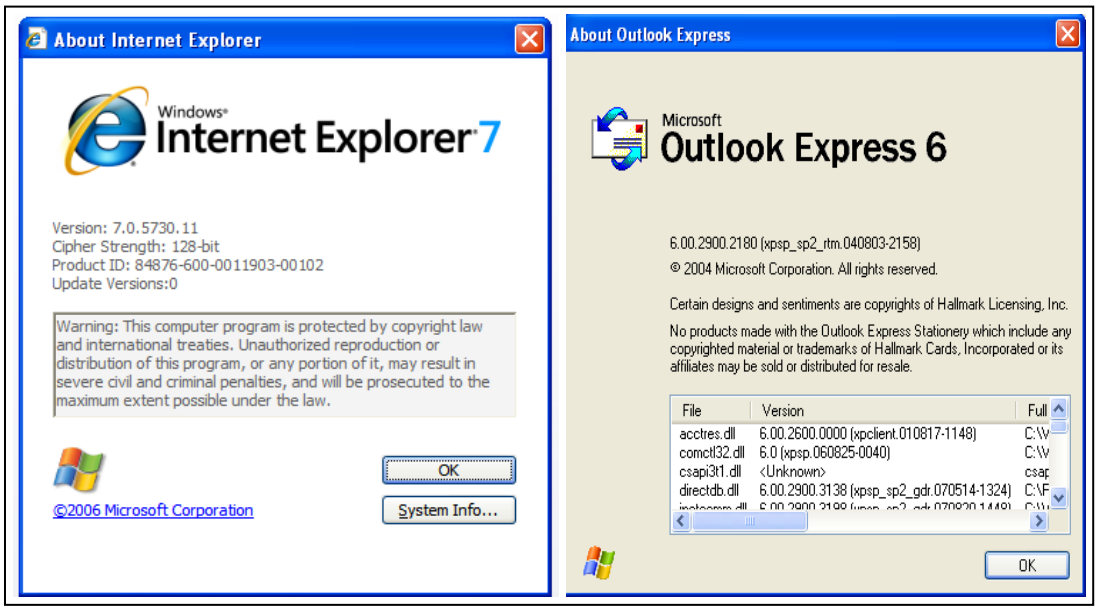
La empresa utiliza el Internet Explorer 7 como navegador web, el cual es una aplicación software que permite al usuario recuperar y visualizar documentos de hipertexto, comúnmente descritos en HTML, desde servidores web de todo el mundo a través de la red de Internet. Esta red de documentos es denominada World Wide Web (WWW). Cualquier navegador actual permite mostrar o ejecutar gráficos, secuencias de vídeo, sonido, animaciones y programas diversos además del texto y los hipervínculos o enlaces.

La funcionalidad básica del navegador web es permitir la visualización de documentos de texto, posiblemente con recursos multimedia incrustados. Los

documentos pueden estar ubicados en la computadora en donde está el usuario, pero también pueden estar en cualquier otro dispositivo que esté conectado a la computadora del usuario o a través de Internet y que tenga los recursos necesarios para la transmisión de los documentos (un software servidor web). Tales documentos, comúnmente denominados páginas web, poseen hipervínculos que enlazan una porción de texto o una imagen a otro documento, normalmente relacionado con el texto o la imagen.

Por otro lado, el programa de mensajería utilizado por la empresa es el Outlook Express 6, el cual permite el envío y recepción de mensajes sobre el Internet a un destinatario externo con el propósito de intercambiar mensajes, archivos, documentos, entre otros, agilitando la comunicación para la organización.

Figura 14. Navegador web y correo electrónico

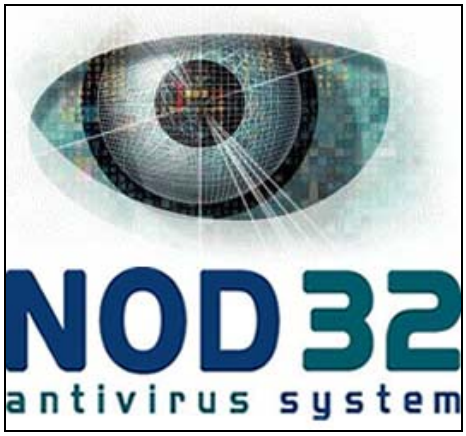


3.2.2.3.3 Antivirus NOD32

Es un programa cuya finalidad es prevenir y evitar la infección de virus, gusanos y troyanos, impidiendo también su propagación.

Tiene capacidad para detectar y eliminar los virus y restaurar los archivos afectados por su infección (en principio).

Figura 15. Antivirus NOD 32



3.3 Identificación de riesgos informáticos

Una vez que hemos efectuado el levantamiento y análisis correspondiente al hardware y software que dispone SAFEGUARD CIA. LTDA., se hace necesario identificar y enlistar cada uno de los riesgos existentes, clasificados de acuerdo a su categoría.

3.3.1 Riesgos de hardware

Al analizar la estructura de hardware definida en la empresa, se ha logrado determinar los riesgos que específicamente en la empresa SAFEGUARD representan una posible amenaza y podrían repercutir en pérdidas no solo económicas sino de diversas índoles; dichos riesgos se detallan a continuación:

- Cortocircuito en el sistema eléctrico
- Daño de las baterías de respaldo (UPS)
- Daño de las interfaces de salida (impresoras, monitores, etc)
- Desastres naturales
- Falla humana en instalaciones y mantenimientos
- Fallas en el software
- Fallos en discos duros del servidor y computadores
- Interrupción del suministro de energía eléctrica
- Pérdida de conexión de la Red
- Robo de equipos

- Vandalismo y destrucción
- Variación de voltaje en la red eléctrica

3.3.2 Riesgos de software

Por otra parte, se ha procedido con la identificación de riesgos al software que posee la empresa en su conjunto, es decir, se los ha clasificado por cada sistema informático, ya que todos se encuentran vinculados y permiten el funcionamiento del sistema informático contable que es nuestro tema de estudio.

3.3.2.1 Riesgos del sistema contable

Luego de analizar el software contable y considerando que es el tema central de nuestro estudio, hemos identificado los siguientes riesgos:

- Acceso al sistema sin autorización
- Crackers
- Error interno del sistema (error en validación)
- Fallas humanas en ingreso de información al sistema
- Fallo de hardware
- Fallos del sistema operativo
- Fallos internos en la estructura del sistema (errores de programación)
- Gusanos y troyanos
- Hackers
- Inconsistencia en información
- Robo de información
- Spyware
- Virus

3.3.2.2 Riesgos del sistema operativo

Como ya se ha expuesto anteriormente, el análisis de los riesgos existentes en el sistema operativo resulta de vital importancia y no los podemos pasar por alto por

cuanto el mismo actúa como plataforma para el funcionamiento del software contable; de esta manera se han identificado los siguientes riesgos:

- Actualizaciones del sistema indebidas
- Afectación de virus
- Crackers
- Daño del sistema
- Eliminación de archivos del sistema
- Fallo del hardware
- Gusanos y troyanos
- Hackers
- Ingresos no autorizados al sistema
- Instalación indebida de programas
- Spyware

3.3.2.3 Riesgos de las herramientas informáticas

Finalmente, efectuamos el análisis a los diversos sistemas de herramientas informáticas, los cuales van de la mano con las necesidades de la empresa y por ende del departamento contable, dentro del cual hemos identificado los siguientes riesgos:

- Acceso a contenidos inapropiados
- Fallo del hardware
- Phishing
- Robo de información
- Spam (correo electrónico basura)
- Virus /macros

3.3.3 Medidas de control de riesgos existentes en la empresa

Con la finalidad de determinar cuáles son las actuales medidas de control que maneja la empresa, se elaboró un cuestionario de 37 preguntas (*Anexo 1*), las mismas que cubren varias áreas de la empresa y que están relacionadas con los sistemas informáticos.

En base a los resultados obtenidos a partir de dicha encuesta se pretende sugerir la reestructuración e implementación de nuevas medidas de control de riesgos; dichas sugerencias serán analizadas posteriormente dentro del informe de hallazgos y recomendaciones.

La encuesta fue efectuada al responsable del departamento de tecnologías y al jefe operativo, luego de lo cual se procede a describir las medidas de control existentes, las cuales se detallan a continuación:

- A nivel de hardware la empresa cuenta con personal de vigilancia que custodia las instalaciones las 24 horas en turnos rotativos.
- Se lleva el control del personal que ingresa y se registra en el libro de novedades.
- Los procedimientos de seguridad son de conocimiento de los usuarios de los sistemas.
- El encargado de la parte de tecnologías es quien administra y asigna a los usuarios los atributos de acuerdo al perfil del mismo.
- La empresa dispone de dispositivos de seguridad física y electrónica como son: alarma, sistema de CCTV, extintores, luces de señalización y señales auditivas.
- A nivel de software se dispone de sistemas originales, los mismos que tienen los respaldos y actualizaciones necesarias al igual que antivirus y sistemas de seguridad de software.

3.4 Calificación de riesgos informáticos encontrados

Una vez identificados los riesgos existentes tanto en el hardware como en el software contable de la empresa, se hace necesario calificar cada uno de ellos en base a la probabilidad de ocurrencia y nivel de impacto que ocasionarían en caso de llegar a materializarse, para posteriormente proceder a priorizarlos y emitir las recomendaciones correspondientes.

La puntuación asignada a cada riesgo dentro de este proceso es valorada conjuntamente con el jefe de tecnologías y jefe operativo, así como mediante la

observación propia a los sistemas informáticos y a la infraestructura física de la empresa como son: equipos, instalaciones, conexiones de red y demás recursos que se relación con los sistemas informáticos contables.

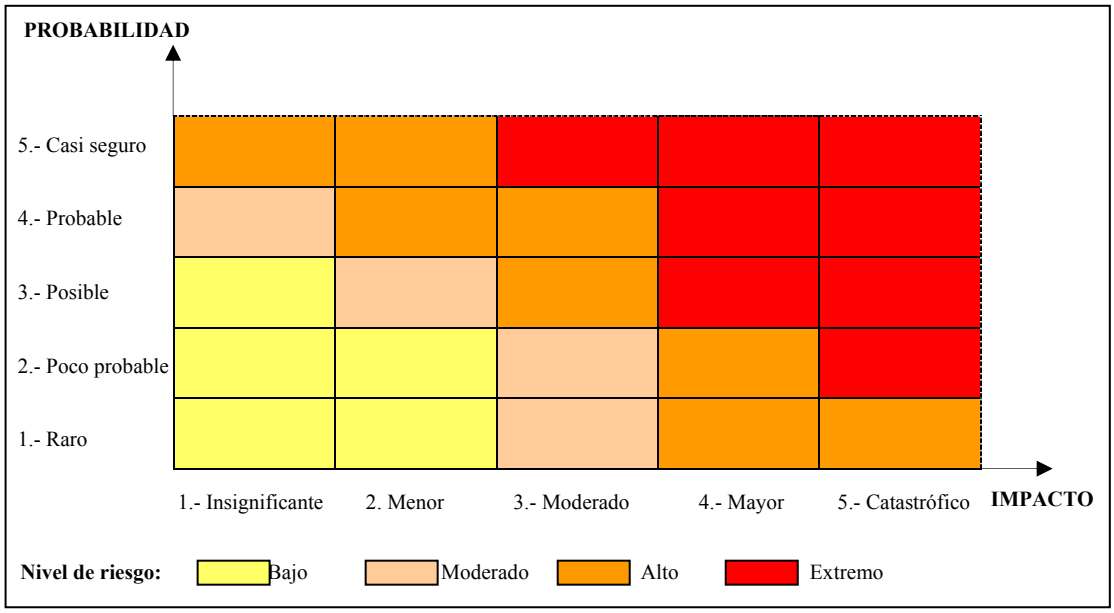
Para tal efecto nos basaremos en el Cuadro 1, el cual nos indica los niveles de probabilidad e impacto para aplicarlas al proceso de calificación:

Cuadro 1. Niveles de probabilidad e impacto de los riesgos

NIVEL	PROBABILIDAD	IMPACTO
1	Raro	Insignificante
2	Poco probable	Menor
3	Posible	Moderado
4	Probable	Mayor
5	Casi seguro	Catastrófico

Luego de calificados los riesgos, se procede a representarlos gráficamente en una matriz de riesgos (Gráfico 1) para determinar su nivel de gravedad y proceder a priorizarlos.

Grafico 1. Mapa de riesgos



En el mapa de riesgos descrito en el Gráfico 1 debemos ubicar cada uno de los riesgos identificados, pudiendo considerarse en varios niveles, cuyo tratamiento lo detallamos a continuación:

Cuadro 2. Niveles de riesgo y tratamiento a considerar

Nivel de riesgo	Tratamiento
Extremo	Representa un grave peligro, requiere medidas de tratamiento inmediatas
Alto	Medidas de tratamiento a corto plazo
Moderado	Medidas de tratamiento a largo plazo
Bajo	No representa peligro y no requiere medidas de tratamiento a corto plazo

Todos los parámetros descritos anteriormente serán utilizados tanto en la calificación de los riesgos de hardware como en la de software.

3.4.1 Calificación de riesgos de hardware

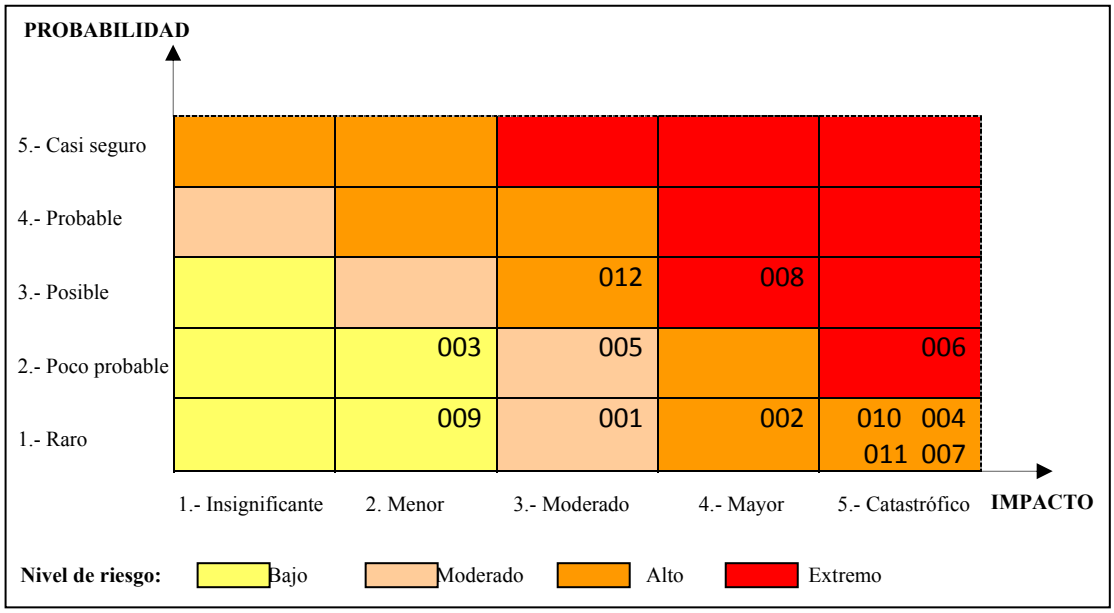
En el presente análisis procedemos a calificar los riesgos identificados a nivel del hardware de contabilidad; dicha calificación viene dada según el Cuadro 3.

Cuadro 3. Calificación de riesgos detectados en hardware

No.	Riesgo	Probabilidad	Impacto	Valor	Nivel
001	Cortocircuito en el sistema eléctrico	1	3	3	Moderado
002	Daño de las baterías de respaldo (UPS)	1	4	4	Alto
003	Daño de las interfaces de salida (impresoras, monitores, etc)	2	2	4	Bajo
004	Desastres naturales	1	5	5	Alto
005	Falla humana en instalaciones y mantenimientos	2	3	6	Moderado
006	Fallos en discos duros del servidor y computadores	2	5	10	Extremo
007	Incendio	1	5	5	Alto
008	Interrupción del suministro de energía eléctrica	3	4	12	Extremo
009	Pérdida de conexión de la Red	1	2	2	Bajo
010	Robo de equipos	1	5	5	Alto
011	Vandalismo y destrucción	1	5	5	Alto
012	Variación de voltaje en la red eléctrica	3	3	9	Alto

A partir de este análisis procedemos a representarlos de manera gráfica y ubicarlos en el cuadrante correspondiente de acuerdo al nivel de riesgo obtenido (Gráfico 2).

Grafico 2. Mapa de riesgos de hardware



3.4.2 Calificación de riesgos del sistema contable

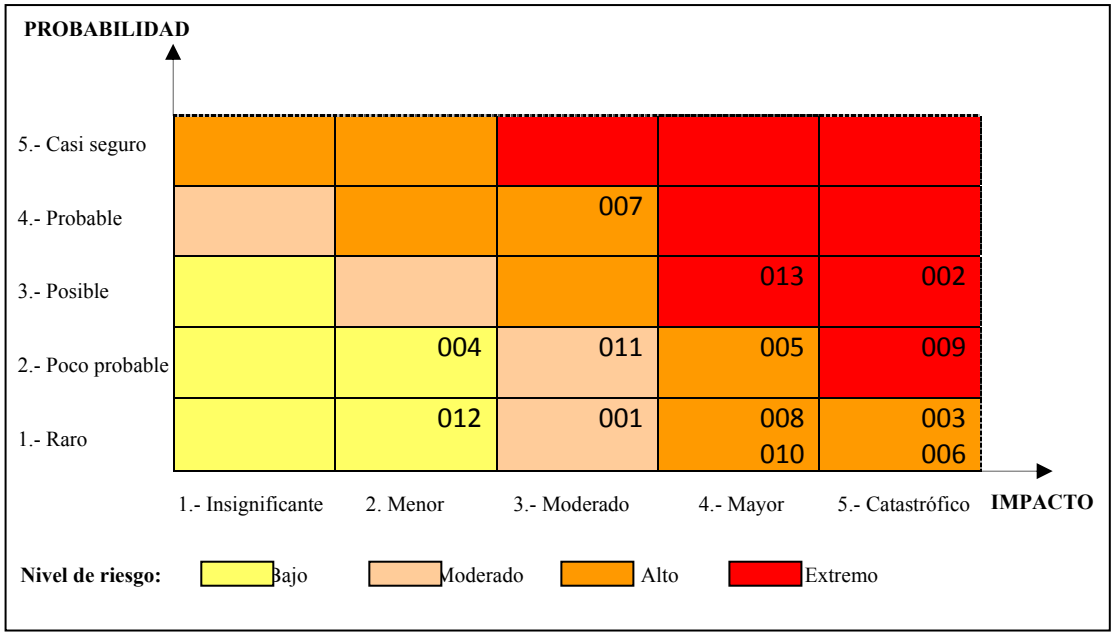
Una vez calificados los riesgos de hardware, es procedente calificar aquellos asociados a los sistemas informáticos, para lo cual iniciaremos con el software contable ya que es el más importante por tratarse de nuestro tema de estudio; dicha calificación la presentamos a continuación:

Cuadro 4. Calificación de riesgos detectados en el sistema contable

No.	Riesgo	Probabilidad	Impacto	Valor	Nivel
001	Crackers	1	3	3	Moderado
002	Fallo de hardware	3	5	15	Extremo
003	Error interno del sistema (error en validación)	1	5	5	Alto
004	Fallas humanas en ingreso de información al sistema	2	2	4	Bajo
005	Fallos del sistema operativo	2	4	8	Alto
006	Fallos internos en la estructura del sistema (errores de programación)	1	5	5	Alto
007	Gusanos y troyanos	4	3	12	Alto
008	Hackers	1	4	4	Alto
009	Inconsistencia en información	2	5	10	Extremo
010	Acceso al sistema sin autorización	1	4	4	Alto
011	Robo de información	2	3	6	Moderado
012	Spyware	1	2	2	Bajo
013	Virus	3	4	12	Extremo

De la misma manera, representamos de manera gráfica la calificación:

Grafico 3. Mapa de riesgos del sistema contable



3.4.3 Calificación de riesgos del sistema operativo

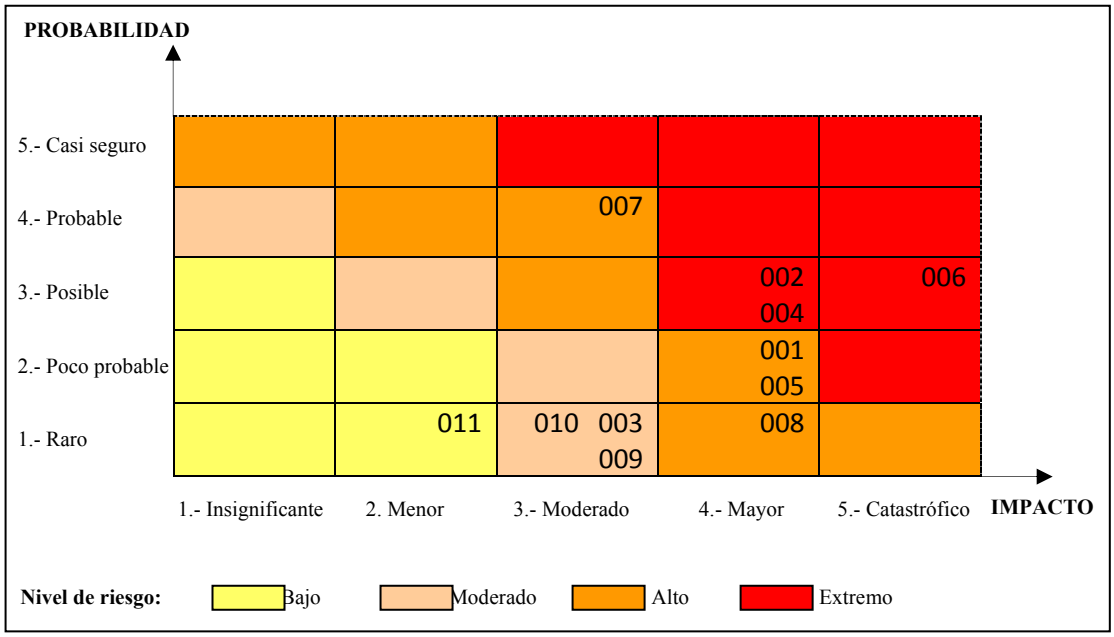
La probabilidad e impacto asignados a los riesgos del sistema operativo ha sido evaluada como sigue:

Cuadro 5. Calificación de riesgos detectados en el sistema operativo

No.	Riesgo	Probabilidad	Impacto	Valor	Nivel
001	Actualizaciones del sistema indebidas	2	4	8	Alto
002	Afectación de virus	3	4	12	Extremo
003	Crackers	1	3	3	Moderado
004	Daño del sistema	3	4	12	Extremo
005	Eliminación de archivos del sistema	2	4	8	Alto
006	Fallo del hardware	3	5	15	Extremo
007	Gusanos y troyanos	4	3	12	Alto
008	Hackers	1	4	4	Alto
009	Ingresos no autorizados al sistema	1	3	3	Moderado
010	Instalación indebida de programas	1	3	3	Moderado
011	Spyware	1	2	2	Bajo

La representación gráfica de dicha calificación se la representa en el siguiente mapa de riesgos:

Grafico 4. Mapa de riesgos de l sistema operativo



3.4.4 Calificación de riesgos en herramientas informáticas

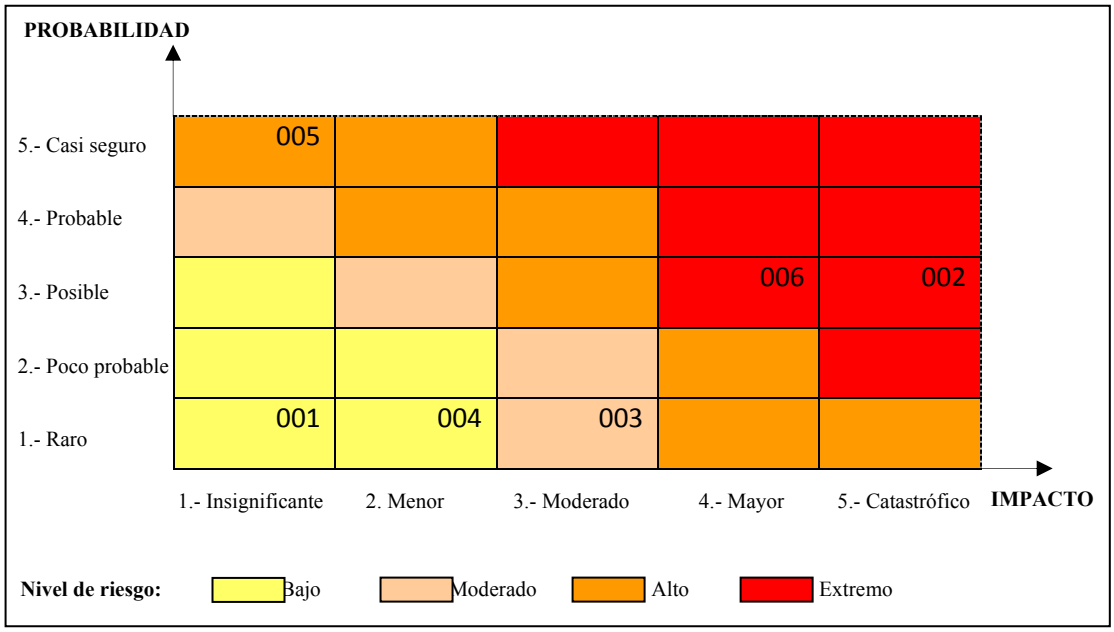
En el cuadro 6 se detalla la calificación asignada a los riesgos detectados en los sistemas de herramientas informáticas que ya fueron definidos anteriormente y que la empresa utiliza de manera conjunta con el software de contabilidad; dicha calificación es la siguiente:

Cuadro 6. Calificación de riesgos detectados en herramientas informáticas

No.	Riesgo	Probabilidad	Impacto	Valor	Nivel
001	Acceso a contenidos inapropiados	1	1	1	Bajo
002	Fallo del hardware	3	5	15	Extremo
003	Phishing	1	3	3	Moderado
004	Robo de información	1	2	2	Bajo
005	Spam (correo electrónico basura)	5	1	5	Alto
006	Virus /macros	3	4	12	Extremo

Dicha calificación se ve plasmada en el mapa de riesgos que se detalla a continuación:

Grafico 5. Mapa de riesgos de las herramientas informáticas



3.5 Asignación de prioridades a los riesgos detectados

En base a la calificación anteriormente efectuada tanto en hardware como en software contable, procedemos a priorizar los riesgos según su nivel de riesgo, de esta manera podremos conocer cuáles son los más relevantes o peligrosos para la organización y por ende recomendar su gestión de manera prioritaria.

3.5.1 Asignación de prioridades a los riesgos de hardware

Una vez identificados y calificados los riesgos existentes en el hardware contable de la organización, fácilmente podemos priorizarlos según el nivel de riesgo obtenido a partir del mapa de riesgos respectivo, de manera que el orden de prioridad a considerar es el siguiente:

Cuadro 7. Asignación de prioridades a los riesgos de hardware

Orden de prioridad	Riesgo	Nivel de riesgo	Valor según calificación
1	Interrupción del suministro de energía eléctrica	Extremo	12
2	Fallos en discos duros del servidor y computadores	Extremo	10
3	Variación de voltaje en la red eléctrica	Alto	9
4	Desastres naturales	Alto	5
5	Incendio	Alto	5
6	Robo de equipos	Alto	5
7	Vandalismo y destrucción	Alto	5
8	Daño de las baterías de respaldo (UPS)	Alto	4
9	Falla humana en instalaciones y mantenimientos	Moderado	6
10	Cortocircuito en el sistema eléctrico	Moderado	3
11	Daño de las interfaces de salida (impresoras, monitores, etc)	Bajo	4
12	Pérdida de conexión de la Red	Bajo	2

3.5.2 Asignación de prioridades a los riesgos del sistema contable

Para el caso de los riesgos existentes en el sistema contable la priorización de los mismos viene dada de la siguiente manera:

Cuadro 8. Asignación de prioridades a los riesgos del sistema contable

Orden de prioridad	Riesgo	Nivel de riesgo	Valor según calificación
1	Fallo de hardware	Extremo	15
2	Virus	Extremo	12
3	Inconsistencia en información	Extremo	10
4	Gusanos y troyanos	Alto	12
5	Fallos del sistema operativo	Alto	8
6	Error interno del sistema (error en validación)	Alto	5
7	Fallos internos en la estructura del sistema (errores de programación)	Alto	5
8	Hackers	Alto	4
9	Acceso al sistema sin autorización	Alto	4
10	Robo de información	Moderado	6
11	Crackers	Moderado	3
12	Fallas humanas en ingreso de información al sistema	Bajo	4
13	Spyware	Bajo	2

3.5.3 Asignación de prioridades a los riesgos del sistema operativo

Por otra parte procedemos a categorizar y priorizar los riesgos del sistema operativo que posee el área contable de la empresa, estos son los siguientes:

Cuadro 9. Asignación de prioridades a los riesgos del sistema operativo

Orden de prioridad	Riesgo	Nivel de riesgo	Valor según calificación
1	Fallo del hardware	Extremo	15
2	Afectación de virus	Extremo	12
3	Daño del sistema	Extremo	12
4	Gusanos y troyanos	Alto	12
5	Actualizaciones del sistema indebidas	Alto	8
6	Eliminación de archivos del sistema	Alto	8
7	Hackers	Alto	4
8	Crackers	Moderado	3
9	Ingresos no autorizados al sistema	Moderado	3
10	Instalación indebida de programas	Moderado	3
11	Spyware	Bajo	2

3.5.4 Asignación de prioridades a los riesgos de herramientas informáticas

Finalmente, el orden prioritario que poseen los riesgos de los sistemas que forman parte de las herramientas informáticas es el siguiente:

Cuadro 10. Asignación de prioridades a los riesgos de herramientas informáticas

Orden de prioridad	Riesgo	Valor según calificación	Nivel de riesgo
1	Fallo del hardware	Extremo	15
2	Virus /macros	Extremo	12
3	Spam (correo electrónico basura)	Alto	5
4	Phishing	Moderado	3
5	Robo de información	Bajo	2
6	Acceso a contenidos inapropiados	Bajo	1

3.6 Elaboración del informe de hallazgos y recomendaciones

Una vez evaluados los riesgos informáticos detectados en el hardware y software contable de la empresa, se procede con la elaboración del informe de hallazgos con sus respectivas recomendaciones para presentarlo a la junta general de accionistas de la compañía; dicho informe viene dado de la siguiente manera:

INFORME DE HALLAZOS Y RECOMENDACIONES DE LA EVALUACION DE RIESGOS INFORMATICOS AL SISTEMA CONTABLE DE LA EMPRESA SAFEGUARD CIA. LTDA.

OFICIO: 001
ASUNTO: Comunicación de resultados y recomendaciones
FECHA: Cuenca, 17 de Julio de 2008

Señores
JUNTA GENERAL DE ACCIONISTAS
Ciudad

De nuestras consideraciones:

La presente tiene como objeto dar a conocer a ustedes que la Evaluación de Riesgos Informáticos al Sistema Informático Contable de la empresa SAFEGUARD CIA. LTDA., fue analizada en el período comprendido entre el 01 de junio y el 15 julio de 2008, tiempo que permitió cumplir con los objetivos propuestos.

Luego de la evaluación realizada podemos destacar que la empresa SAFEGUARD CIA. LTDA. mantiene ciertas medidas de control para los riesgos informáticos, sin embargo se pudo determinar que no son ejecutadas a cabalidad, por lo que se hace necesario reestructurar e implementar nuevos mecanismos de control de riesgos.

El proceso de evaluación llevado a cabo fue aplicado a nivel de hardware y software del área informática contable de la empresa, dentro de este último hemos analizado no solo el sistema de contabilidad sino también el sistema operativo y herramientas informáticas ya que se encuentran relacionadas entre sí y funcionan conjuntamente.

Los cuadros a continuación detallan los riesgos detectados en el hardware y software en orden de prioridad según su nivel de riesgo, así como las medidas de control existentes y las medidas de tratamiento sugeridas que consideramos necesarias en la empresa a partir de las falencias detectadas:

Cuadro 1. Hallazgos y recomendaciones en riesgos de hardware

Orden de prioridad	Riesgo	Nivel de riesgo	Control existente	Medida de tratamiento sugerida
1	Interrupción del suministro de energía eléctrica	Extremo	Se cuenta con baterías de respaldo (UPS) para el servidor	Implementación de un generador eléctrico que suministre energía por períodos prolongados de tiempo
2	Fallos en discos duros del servidor y computadores	Extremo	Se efectúan respaldos periódicos de información	Implementación de un RIDE de discos para tener de manera redundante la información a manera de espejo
3	Variación de voltaje en la red eléctrica	Alto	Ninguna	Implementar reguladores de voltaje
4	Desastres naturales	Alto	Pólizas de seguro	Mantener la póliza y renovarla permanentemente
5	Incendio	Alto	Pólizas de seguro	Mantener la póliza y renovarla permanentemente
			Extintores	Capacitar al personal en el manejo y uso de los extintores y mantenerlos en buen estado
6	Robo de equipos	Alto	Pólizas de seguro	Mantener la póliza y renovarla permanentemente
			Seguridad física y electrónica	Mantener
7	Vandalismo y destrucción	Alto	Pólizas de seguro	Mantener la póliza y renovarla permanentemente
			Seguridad física	Mantener
8	Daño de las baterías de respaldo (UPS)	Alto	Mantenimiento periódico	Mantener
9	Falla humana en instalaciones y mantenimientos	Moderado	Se realizan pruebas posteriores	Capacitar al personal técnico y determinar un supervisor de los trabajos realizados
10	Cortocircuito en el sistema eléctrico	Moderado	Pólizas de seguro	Mantener la póliza y renovarla permanentemente
11	Daño de las interfaces de salida (impresoras, monitores, etc)	Bajo	Mantenimiento periódico	Mantener
12	Pérdida de conexión de la Red	Bajo	Monitoreo permanente de la señal	Mantener

Cuadro 2. Hallazgos y recomendaciones en riesgos del sistema contable

Orden de prioridad	Riesgo	Nivel de riesgo	Control existente	Medida de tratamiento sugerida
1	Fallo de hardware	Extremo	Se mantienen respaldos en medio magnético	Mantener
2	Virus	Extremo	Antivirus	Actualizaciones automáticas a través de Internet y llevar un registro
3	Inconsistencia en información	Extremo	Validación de la información de forma manual	Mantener
4	Gusanos y troyanos	Alto	Antivirus	Actualizaciones automáticas a través de Internet y llevar un registro
5	Fallos del sistema operativo	Alto	Se crean puntos de restauración del sistema	Mantener el procedimiento existente y adicionalmente respaldar la información
6	Error interno del sistema (error en validación)	Alto	Validación de la información de forma manual	Mantener
7	Fallos internos en la estructura del sistema (errores de programación)	Alto	Garantía y soporte técnico del proveedor	Mantener el procedimiento y renovar el soporte técnico permanentemente
8	Hackers	Alto	Firewall y sistemas de monitoreo y protección	Mantener y actualizar versiones de software
9	Acceso al sistema sin autorización	Alto	Asignación de responsabilidades	Promover la ética y moral entre los usuarios
			Respaldo de accesos en históricos	Mantener
10	Robo de información	Moderado	Asignación de responsabilidades	Promover la ética y moral entre los usuarios
11	Crackers	Moderado	Firewall y sistemas de monitoreo y protección	Mantener y actualizar versiones de software
12	Fallas humanas en ingreso de información al sistema	Bajo	Validación manual de información ingresada	Capacitar al personal en manejo de información
13	Spyware	Bajo	Firewall y sistemas de monitoreo y protección	Mantener y actualizar versiones de software

Cuadro 3. Hallazgos y recomendaciones en riesgos del sistema operativo

Orden de prioridad	Riesgo	Nivel de riesgo	Control existente	Medida de tratamiento sugerida
1	Fallo del hardware	Extremo	Se mantienen respaldos en medio magnético	Mantener
2	Afectación de virus	Extremo	Antivirus	Actualizaciones automáticas a través de Internet y llevar un registro
3	Daño del sistema	Extremo	Se crean puntos de restauración del sistema	Mantener el procedimiento existente y adicionalmente respaldar la información
4	Gusanos y troyanos	Alto	Antivirus	Actualizaciones automáticas a través de Internet y llevar un registro
5	Actualizaciones del sistema indebidas	Alto	Solo el administrador del sistema tiene acceso	Mantener
6	Eliminación de archivos del sistema	Alto	Se mantiene respaldo de la información	Capacitar a los usuarios para prevenir la eliminación de archivos
7	Hackers	Alto	Firewall y sistemas de monitoreo y protección	Mantener y actualizar versiones de software
8	Crackers	Alto	Firewall y sistemas de monitoreo y protección	Mantener y actualizar versiones de software
9	Ingresos no autorizados al sistema	Alto	Asignación de responsabilidades	Promover la ética y moral entre los usuarios
			Respaldo de accesos en históricos	Mantener
10	Instalación indebida de programas	Moderado	Solo el administrador del sistema tiene acceso	Mantener
11	Spyware	Moderado	Firewall y sistemas de monitoreo y protección	Mantener y actualizar versiones de software

Cuadro 4. Hallazgos y recomendaciones en riesgos de herramientas informáticas

Orden de prioridad	Riesgo	Nivel de riesgo	Control existente	Medida de tratamiento sugerida
1	Fallo del hardware	Extremo	Se mantienen respaldos en medio magnético	Mantener
2	Virus /macros	Extremo	Antivirus	Actualizaciones automáticas a través de Internet y llevar un registro
3	Spam (correo electrónico basura)	Alto	Existen filtros de bloqueo de correo no deseado	Mantener
4	Phishing	Moderado	El navegador está configurado para bloquear sitios web no seguros	Capacitar al personal para reconocer sitios no seguros
5	Robo de información	Bajo	Asignación de responsabilidades	Mantener
6	Acceso a contenidos inapropiados	Bajo	El navegador está configurado para bloquear sitios web no seguros	Capacitar al personal para reconocer sitios no seguros

Para la implementación de las medidas de seguridad que hemos sugerido, es necesario que se considere la prioridad que fue asignada a cada uno de los riesgos en función de su nivel, para de esta manera determinar qué riesgos deben ser gestionados inmediatamente; el tratamiento sugerido en función del nivel de riesgo viene dado por el siguiente cuadro:

Cuadro 5. Niveles de riesgo

Nivel de riesgo	Tratamiento
Extremo	Representa un grave peligro, requiere medidas de tratamiento inmediatas
Alto	Medidas de tratamiento a corto plazo
Moderado	Medidas de tratamiento a largo plazo
Bajo	No representa peligro y no requiere medidas de tratamiento a corto plazo

Esperando que la presente evaluación tenga como objeto gestionar los riesgos de manera efectiva y fortalecer la seguridad en los sistemas informáticos del área contable.

Atentamente,

Ing. Rodrigo Cruz Sr. Freddy Vidal

3.7 Conclusiones del capítulo

En el transcurso del presente capítulo se procedió a evaluar los riesgos informáticos existentes en el sistema contable de la empresa de manera práctica, para lo cual fueron evaluados adicionalmente aquellos provenientes del hardware, sistema operativo y herramientas informáticas, ya que se encuentran relacionados entre sí y permiten el funcionamiento del sistema contable, el cual es nuestro tema de estudio.

Los procedimientos de evaluación empleados en este capítulo tienen su base conceptual en el módulo de riesgos informáticos recibidos en el curso de graduación; de esta manera se realizó un análisis previo a la estructura de hardware y software con la que cuenta el área contable de la empresa, luego de lo cual se identificaron cada uno de los riesgos existentes en los mismos; adicional a ello se procedió a efectuar una encuesta al jefe de tecnologías y jefe operativo que permitió determinar la existencia de ciertos controles a los riesgos informáticos y a su vez las falencias que permitieron tener una idea clara sobre las amenazas latentes.

Posteriormente se procedió con la calificación y priorización de los riesgos para concluir con la elaboración del informe de hallazgos y recomendaciones dirigidas a la junta general de accionistas de la empresa para su análisis y posterior implementación.

CONCLUSIONES

En la actualidad uno de los activos más valiosos que poseen las empresas es la información que es generada en sus sistemas informáticos, la misma que es considerada como una herramienta para la toma de decisiones.

Es así que para SAFEGUARD CIA. LTDA., una empresa ecuatoriana dedicada a la seguridad privada en las áreas física y electrónica, es de vital importancia mantenerse a la vanguardia a nivel tecnológico con el único propósito de dar el mejor servicio que el cliente merece, por ello vio la necesidad de adquirir hardware y software de acuerdo a sus necesidades, tal es el caso del sistema SOFI, en donde se lleva registro de toda la actividad contable que es ingresada, procesada en sus diferentes módulos y almacenada en sus base de datos, facilitando así la consulta y garantizando que la información que se maneja sea veraz y oportuna.

Cabe resaltar que para el correcto funcionamiento del sistema contable es de crucial importancia disponer de un sistema operativo compatible y con las herramientas necesarias que interactúen de manera armónica con el hardware. Es así que para evaluar los riesgos informáticos contables en la empresa SAFEGUARD CIA. LTDA., se deben tomar en cuenta todos los aspectos tanto de hardware, software y el personal que labora en la misma, pues sin el ser humano, las máquinas no pueden actuar de manera autónoma en la toma de decisiones.

Para iniciar con el proceso de evaluación de riesgos, se realizó un análisis previo a la estructura de hardware y software con la que cuenta el área contable de la empresa, luego se identificaron cada uno de los riesgos existentes en los mismos; adicional a ello se procedió a efectuar una encuesta al jefe de tecnologías y jefe operativo, como conclusión pudimos determinar la existencia de ciertos controles a los riesgos informáticos y de esta manera tener una idea clara sobre las amenazas latentes en el sistema informático contable de la organización.

Posteriormente se procedió con la calificación y priorización de los riesgos para concluir con la elaboración del informe de hallazgos y recomendaciones dirigidas a la junta general de accionistas de la empresa para su análisis y posterior

implementación, y de esta manera cumplir con el objetivo principal planteado al inicio del presente trabajo.

RECOMENDACIONES

Al culminar el trabajo de evaluación de riesgos informáticos al sistema contable de la empresa SAFEGUARD CIA. LTDA., es necesario resaltar algunos puntos de importancia como medida de tratamiento ante la presencia de posibles riesgos que de llegar a materializarse causarían un impacto significativo para la empresa, razón por la cual se hace necesario recomendar a la junta directiva los siguientes puntos.

A nivel de hardware:

- Sugerimos la implementación de generadores eléctricos, los mismos que suministren energía por períodos prolongados de tiempo con el fin de no tener interrupciones del sistema por cortes de energía eléctrica inesperados.
- La implementación de un RIDE (arreglo de discos), garantizando que la información esté disponible en caso de fallo del disco primario.
- Llevar un control permanente de las pólizas de seguro y mantener actualizado el contrato.
- Capacitar y familiarizar al personal de acuerdo a su perfil, con el manejo de los equipos.

A nivel de software:

- Llevar un control de los programas instalados, actualizaciones, modificaciones y eliminación, detallando todos los pormenores que llevaron a realizar esa actividad con el propósito de llevar un registro de cada equipo.
- Respaldar la información de acuerdo a los horarios y fechas establecidas.
- Mantener la red libre de virus, troyanos y demás software malicioso que afecte el desempeño de los equipos.
- Capacitar al personal con el manejo del sistema operativo, utilitarios, herramientas y principalmente con el sistema de contabilidad, garantizando de esta manera que la información que ingresa sea la más adecuada y veraz posible.
- Fomentar la ética y moral entre los funcionarios de la empresa, creando un ambiente propicio de compañerismo y de lealtad.

BIBLIOGRAFIA

Libros

ALVAREZ. Gonzalo — **Seguridad Informática para Empresas y Particulares** 1ª Edic. McGraw-Hill. Interamericana de España S.A.O. 2004

PRESSMAN. Roger — **Ingeniería del Software** 4ª Edic. McGraw-Hill. Madrid. 1998

PRESSMAN. Roger — **Ingeniería del Software** 6ª Edic. McGraw-Hill. México. 2005

VERA. Fernando — **La auditoria interna de la administración de riesgos** 1ª Edic. Instituto Mexicano de Contadores Públicos A.C. México. 1983

Internet

JIMENEZ, José A. — "Evaluación Seguridad de un Sistema de Información". **http://www.monografias.com/trabajos/seguinfo** Junio 2008

RUIZ, Javier — "ISO 27000". España **http://www.iso27000.es/** Junio 2008

IT GOVERNANCE INSTITUTE — **"**COBIT 4.0". Estados Unidos de América **http://www.isaca.org/** Junio 2008

KRAUSE, Micki — "Handbook of Information Security Management" **http://www.cccure.org/Documents/HISM/ewtoc.html** Junio 2008

Enciclopedias

SALVAT. **Enciclopedia salvat diccionario**
Tomo 6. SALVAT EDITORES, S.A. España. 1972

ROSENBERG. J. **Diccionario de Administración y Finanzas**
España. 1983.

ANEXOS

ANEXO 1. Encuesta realizada al jefe de tecnologías y jefe operativo