UNIVERSIDAD SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS

EVALUACIÓN CONTROL INTERNO INFORMÁTICO SOBRE LA SEGURIDAD DEL ÁREA DE SISTEMAS DE UNA INDUSTRIA DE CALZADO

TESIS

PRESENTADA A LA JUNTA DIRECTIVA
DE LA FACULTAD DE CIENCIAS ECONÓMICAS

POR

KARIN XIOMARA FIGUEROA DE LA CRUZ

PREVIO A CONFERÍRSELE EL TÍTULO DE

CONTADORA PÚBLICA Y AUDITORA

EN EL GRADO ACADÉMICO DE

LICENCIADA

Guatemala, Septiembre de 2011

MIEMBROS DE LA JUNTA DIRECTIVA
FACULTAD DE CIENCIAS ECONOMICAS

Decano:	Lic. José Rolando Secaida Morales
Secretario:	Lic. Carlos Roberto Cabrera Morales
Vocal Primero:	Lic. M.Sc. Albaro Joel Girón Barahona
Vocal Segundo:	Lic. Mario Leonel Perdomo Salguero
Vocal Tercero:	Lic. Juan Antonio Gómez Monterroso
Vocal Cuarto:	P.C Edgar Arnoldo Quiché Chiyal
Vocal Quinto:	P.C José Antonio Vielman

PROFESIONALES QUE REALIZARON
LOS EXÁMENES DE ÁREAS PRÁCTICAS BÁSICAS

Auditoria:	Lic. Manuel Fernando Morales Garcia
Matemática Estadística:	Lic. Edgar Ranulfo Valdés Castañeda
Contabilidad:	Lic. José Adán De León

PROFESIONALES QUE REALIZARON EL EXAMEN PRIVADO DE TESIS

Presidente:	Lic. Sergio Arturo Sosa Rivas
Secretario:	Lic. Nelton Estuardo Mérida
Examinador:	Lic. Miguel Ángel Lira Trujillo

LICENCIADO CARLOS G. ESCOBAR T.
CONTADOR PÚBLICO Y AUDITOR

Guatemala, 17 de enero 2011

Licenciado
José Rolando Secaída Morales
Decano de la Facultad de Ciencias Económicas
Universidad de San Carlos de Guatemala

Apreciable señor Decano:

Me permito informarle, que he procedido a examinar y asesorar el trabajo de tesis elaborado por la estudiante Karin Xiomara Figueroa De La Cruz, denominado: **"Evaluación Control Interno Informático sobre la Seguridad del área de Sistemas de una Industria de Calzado".**

Considero en base a mi experiencia profesional que, el trabajo de tesis mencionado fue desarrollado tomando en cuenta todos los aspectos necesarios y los requisitos establecidos, además la estudiante tomo en cuenta mis comentarios y sugerencias en el transcurso de la elaboración de su trabajo.

Por lo anterior solicito que se revise por la facultad, el presente trabajo de tesis.

Atentamente,

Lic. Carlos Gilberto Escobar Téllez
Colegiado No. 4144

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE CIENCIAS ECONOMICAS

Edificio "S-8"

Ciudad Universitaria, Zona 12
GUATEMALA, CENTROAMERICA

DECANATO DE LA FACULTAD DE CIENCIAS ECONOMICAS. GUATEMALA, SIETE DE NOVIEMBRE DE DOS MIL ONCE.

Con base en el Punto QUINTO, inciso 5.1, subinciso 5.1.1 del Acta 30-2011 de la sesión celebrada por la Junta Directiva de la Facultad el 31 de octubre de 2011, se conoció el Acta AUDITORIA 197-2011 de aprobación del Examen Privado de Tesis, de fecha 5 de septiembre de 2011 y el trabajo de Tesis denominado: "EVALUACIÓN CONTROL INTERNO INFORMÁTICO SOBRE LA SEGURIDAD DEL ÁREA DE SISTEMAS DE UNA INDUSTRIA DE CALZADO", que para su graduación profesional presentó la estudiante KARIN XIOMARA FIGUEROA DE LA CRUZ, autorizándose su impresión.

Atentamente,

"ID Y ENSEÑAD A TODOS"

LIC. CARLOS ROBERTO CABRERA MORALES
SECRETARIO

FACULTAD DE CIENCIAS ECONOMICAS
EL SECRETARIO
Guatemala, C. A.

LIC. JOSE ROLANDO SECAIDA MORALES
DECANO

FACULTAD DE CIENCIAS ECONOMICAS
EL DECANO
GUATEMALA, C. A.

Smp.

Ingrid

DEDICATORIA

A DIOS: Por brindarme sabiduría y entendimiento para alcanzar esta meta, y porque todo lo puedo en Cristo que me fortalece.

A MIS PADRES: **Jovita De La Cruz y Mario Figueroa (+)**
Quienes con la bendición de Dios me dieron la vida, me formaron y me impulsaron alcanzar mis metas.

A MIS HERMANOS: **Raquel, Evelyn, Marilú y Mario**
Por el amor que nos une y su apoyo incondicional.

A MIS SOBRINOS: **Xiomara, Iván, Pablo, Kevin, Giovanni y Jessy**
Por ser las personitas que me alegran el día.

A MI FAMILIA: Con todo mi cariño.

A MIS AMIGOS: **Blanca, Damaris, Dinora, Glenda, Silvia, Wanda, Hugo, Daniel, Ángel y Ezequiel**
Con quienes hemos compartido gratos momentos y en quienes he encontrado apoyo y ayuda cuando lo he necesitado.

A MI PASTOR: **Lic. Wenceslao Guerra**, por sus consejos y motivación.

A MI PASTOR: **Lic. Wenceslao Guerra**, por sus consejos y motivación.

A MIS ASESORES: **Lic. Carlos Escobar, Lic. Edgar Valdez**
Por el tiempo invertido y haberme apoyado en la realización de esta tesis, gracias.

A LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA: A la que agradezco por la oportunidad de formarme académicamente.

A LA FACULTAD DE CIENCIAS ECONÓMICAS: Muy especialmente.

ÍNDICE

INTRODUCCIÓN

En la actualidad, toda empresa se desarrolla en un ambiente progresivo y competitivo, por lo que se hace necesario tomar decisiones correctas y de forma oportuna. Es por ello que toda herramienta que ayude al empresario a obtener información confiable y segura le resulte ser una ventaja competitiva, tal es el caso de la evaluación del control Interno informático.

El Control Interno constituye un elemento importante sujeto a análisis y evaluación durante un proceso de auditoría, con énfasis en la fase de Planificación, puesto que permite analizar el entorno de la empresa, su organización, ambiente de control, riesgo de negocio, los procedimientos administrativos de control y los sistemas financieros utilizados.

Los sistemas informáticos son tan importantes en la actualidad dado el papel que desempeñan en las empresas, convirtiéndose en herramientas indispensables por el apoyo significativo para la administración en la toma de decisiones importantes que derivan operaciones con efectividad, eficiencia y resultados positivos. No obstante, aún persiste en muchos casos que no se efectúan evaluaciones periódicas o son muy limitadas, sin personal especializado, principalmente en el Departamento de Auditoría Interna.

A través del control interno informático la administración de una empresa busca asegurar que se logren los objetivos previstos, aprobados y se cumpla con las funciones, tareas relacionadas con la previsión, seguimiento y control de su actividad económica, financiera administrativa.

La Auditoría en sistemas es la revisión y evaluación de los controles, métodos y procedimientos establecidos en el Departamento de Sistemas, quien puede mantener una tecnología de punta, contará con apropiados procesos de registro e información vitales para la Gerencia General.

La finalidad del Departamento de Auditoría Interna, es rendir informes certeros y oportunos a la alta administración, cuyos riesgos detectados deben ser objeto de inminentes acciones y medidas de corrección que el auditor considere que permitirán eliminar, reducir o minimizar las causas u origen de las mismas.

La presente tesis ha sido enfocada específicamente en la Evaluación del Control Interno Informático del área de Seguridad del Departamento de Sistemas de una Industria de Calzado, utilizando el método COSO ERM (Gestión del Riesgo Empresarial); la hipótesis busca comprobar las deficiencias en la protección, confiabilidad, pérdida de la información, falta de resguardos, y la inadecuada seguridad en el uso de los equipos.

De las investigaciones y análisis efectuados se logró comprobar la hipótesis por medio del caso práctico.

En el capítulo uno se describe la Industria de Calzado en Guatemala, presentando un breve relato histórico de la misma, su definición, características generales y clasificación del calzado y por último menciona algunas de las leyes de observancia general para las empresas que pertenecen al sector Industrial de Calzado de Guatemala.

El capítulo dos expone la auditoría en sistemas en una Industria de Calzado y describe sus antecedentes, definición, importancia, objetivos, beneficios, funciones y elementos.

El capítulo tres enfoca el control interno informático sobre la seguridad del área de sistemas, describe sus antecedentes, definición, importancia, objetivos, funciones, elementos, el control interno en base al COSO ERM (Gestión del Riesgo Empresarial), métodos, riesgos y su clasificación.

El capítulo cuatro lo constituye el caso práctico, como parte fundamental del trabajo de investigación; asimismo, presenta los lineamientos necesarios para evaluar el control interno informático sobre la seguridad del área de sistemas de una Industria de Calzado.

Finalmente se, presentan las conclusiones y recomendaciones del trabajo realizado.

CAPÍTULO I
EMPRESAS INDUSTRIALES DE CALZADO

1.1 ANTECEDENTES EN GUATEMALA

La utilización de calzado en Guatemala se remonta antes de la venida de los españoles; según la antropóloga Bárbara de Arathon, actualmente investigadora del museo Ixchel del Traje Indígena, las sandalias se constituían como una de las vestimentas de los mayas que habitaron nuestras tierras; esto se visualiza por los tallados en piedra de las estelas, los dibujos en piezas de cerámica, los detalles en los lienzos y en los murales.

Según Adrían Recinos en su traducción del Popol Vuh, libro sagrado de los Quiches, la palabra Xajab del idioma Kaqchikel significa en castellano zapato, sandalia, o caite, de acuerdo al vocablo náhuatl "cactli". (10:1)

Independientemente como haya evolucionado esta palabra, actualmente el calzado indígena de Guatemala varía según la etnia y la región, y el calzado que utiliza la población en general está enmarcado de acuerdo a las corrientes de la moda.

La industria de calzado inició su desarrollo operando bajo la forma de talleres artesanales domésticos utilizando herramientas manuales, por lo que su volumen de producción era relativamente bajo. Posteriormente, debido a la demanda que este producto empezaba a presentar y consecuentemente la necesidad de aumentar la producción, fue necesaria la contratación de un mayor número de trabajadores. (10:1-2)

Con el volumen de producción en los años de 1920 a 1930, aparece en Guatemala un porcentaje alto de producción, concentrado en calzado de campo, elaborado con piel y otras materias primas de uso en ese tiempo. Con la revolución de 1944, las industrias en general recibieron apoyo financiero, originando mayor desarrollo

en la producción y en la especialización de la mano de obra; esto conllevó aplicar la división de trabajo, puesto que cada trabajador se especializó en determinada fase de la elaboración de calzado. En esta etapa las industrias adquirieron maquinaria más tecnificada, lo que permitió obtener una mayor producción a un menor costo.

El desarrollo de estas industrias motivó a muchos empresarios a obtener sus propias materias primas, y fue así como en la década de los años1930 a 1940 surgieron las primeras tenerías que en muchos casos eran propiedad de estas industrias, lo que les permitía obtener materias primas de mejor calidad a menor costo.

En los años, de 1940 a 1950, además de las industrias de calzado de piel, se constituyeron fábricas en Guatemala que se dedicaban a producir calzado deportivo y de hule, diversificándose la producción de calzado lo que originó su crecimiento. A la vez, se promovió un avance en la tecnología para la elaboración de los productos, ya que se requería de materias primas que en algunos casos provenían de otros productos, por ejemplo el hule.

También, en los años de 1950 a 1980, la actividad de calzado se industrializó. El calzado guatemalteco se distinguía por su elegancia, moda y calidad; esto, con la buena economía que la ganadería tenía en ese momento, hizo que se exportara hacia los mercados de Centroamérica y México. El crecimiento de pequeños talleres familiares originó cambios y de ello la transformación a empresas formales con uso de maquinaria de tecnología industrial, pero todavía con ideas de productor artesanal.

Posteriormente, las fábricas iniciaron a producir volúmenes altos de calzado con mejor calidad de materiales, necesarios para una adecuada presentación y aceptación dentro del mercado, ya que los consumidores empezaban a convertirse en clientes más exigentes. (10:3)

Las primeras industrias de calzado instaladas en Guatemala se identificaron como Fábrica de calzado Cobán, Codal, Fábrica Bransy, Fábrica Novelty y Jojivo; posteriormente, surgieron otras fábricas de calzado que penetraron al mercado con una producción en serie que les permitió obtener una variedad de estilos, como altos volúmenes de producción.

En la actualidad, la tendencia de la moda del calzado ha llevado a la utilización de materias primas tales como piel, cuerina, hule, plástico, etc.

1.2 DEFINICIÓN

La industria de calzado es un conjunto de empresas que se dedican a la fabricación de todo tipo de zapato, zapatilla, bota o sandalia con fines de cubrir y proteger el pie. Suele agruparse en la misma rama que la industria de la confección, ya que buena parte se integra al complejo de la industria de la moda. En Guatemala está integrada por un conjunto de pequeñas, medianas y grandes empresas generando un alto porcentaje de puestos de trabajo, siendo un factor determinante para el progreso social y económico del país. (13:3)

1.3 CARACTERÍSTICAS

Las industrias de calzado se caracterizan según su tamaño:

a) Micro, de 1 a 9 empleados; su capacidad de producción es de 100 pares de zapatos por día y con un capital de trabajo menor de Q.50, 000.00.

b) Pequeña, de 10 a 49 empleados; su capacidad de producción es de 101 a 500 pares de zapatos por día y con un capital de trabajo comprendido en el rango de Q 50,001 a Q.500, 000.00.

c) Mediana, de 50 a 99 empleados; su capacidad de producción es de 501 a 1,000.00 pares de zapatos por día y con un capital de trabajo comprendido en el rango de Q.501, 000.00 a Q.2, 000,000.00.

d) Grande, de 100 a más empleados; su producción es mayor a 1,000 pares de zapatos por día con capital de trabajo mayor a Q.2, 000,000.00.

La industria de calzado en Guatemala está conformada aproximadamente por 300 empresas industriales y cinco mil talleres artesanales, que generan gran cantidad de empleos para la población guatemalteca. (13:4)

La ubicación geográfica de estas empresas se distribuye en su mayoría en: Ciudad de Guatemala, Antigua Guatemala, Sacatepéquez, Santa Catarina Mita, Jutiapa, Samayac, Suchitepéquez, Quetzaltenango, Santiago Atitlán, Sololá, San Cristóbal Alta Verapaz y Chiantla Huehuetenango. (13:5)

La producción anual de calzado es alrededor de 39 millones de pares de todo tipo de estilo, teniendo una producción diaria aproximada de 120 mil pares en la industria y 40 mil pares en talleres artesanales; la cual se destina en un 60% para el mercado nacional, 35% para el mercado regional y un 5% para el mercado internacional, siendo los principales países a donde exporta los siguientes (13:8).

a) Centroamérica
b) Panamá
c) México
d) Estados Unidos
e) República Dominicana
f) Cuba

En Guatemala cuando no se cuenta con ciertos insumos para la fabricación del calzado, se importan en su mayoría de los siguientes países (13:8):

a) Estados unidos
b) China
c) El Salvador
d) Brasil
e) Italia
f) México
g) Colombia
h) España

1.4 CLASIFICACIÓN DEL CALZADO

1.4.1 De acuerdo al género

Para dama, caballero y niño.

1.4.2 De acuerdo al material

Piel, tela, lona, yute, materiales sintéticos y otros.

1.4.3 De acuerdo al estilo o tipo de uso

Bota, sandalia, tenis, zapato industrial, zapato de vestir, colegial, pantuflas entre otros. (9:6)

1.5 ASPECTOS LEGALES Y TRIBUTARIOS

Las empresas industriales, comerciales y de servicios ubicadas en la Republica de Guatemala deben cumplir con los requisitos exigidos en el marco de la legislación guatemalteca para operar.

Algunas leyes de observancia general y de cumplimiento obligatorio para las industrias de calzado en Guatemala, se describen a continuación:

a) Constitución Política de la República de Guatemala, establece en su artículo 43, "se reconoce la libertad de industria, de comercio y de trabajo, salvo las limitaciones que por motivos sociales o de interés nacional impongan las leyes."

b) Código de Comercio, Decreto número 2-70 emitido por el Congreso de la República de Guatemala. Dependiendo del tipo de actividad y de la forma de constitución, establece los procedimientos a seguir para obtener la autorización del Registro Mercantil para ejercer el comercio y lo relativo a las obligaciones que todo comerciante debe cumplir como tal.

c) Código Tributario, Decreto número 6-91 el cual establece principalmente, la obligación de inscribirse ante la Administración Tributaría, así como también las sanciones aplicables a todo contribuyente por el incumplimiento de las obligaciones establecidas en las leyes tributarías.

d) Código de Trabajo 1441, vigente desde el 16 de agosto de 1961. En el cual se establecen todas las normas que regulan las relaciones entre patronos y trabajadores.

e) Ley del Impuesto al Valor Agregado y sus reformas (Decreto Número 27-92) El Impuesto al Valor Agregado (IVA) es un gravamen indirecto que se origina, entre otras cosas, en la venta o permuta de bienes y la prestación de servicios, importaciones, arrendamientos, adjudicaciones, retiro de bienes de las empresas (para uso personal), la venta o permuta de bienes inmuebles, la donación entre vivos de bienes muebles e inmuebles y la pérdida de mercadería o cualquier hecho que implique faltantes de inventario.

Por la naturaleza mercantil de la empresa distribuidora de calzado, como adquirientes de bienes y servicios, ya sea que los mismos sean de producción nacional o procedan de otros países (importaciones), está afecta al pago de este impuesto. El tipo impositivo vigente es del 12% sobre los bienes que se comercialicen.

El IVA se paga cuando se realiza la compra de un bien o servicio; dado que el precio incluye el IVA, si no se emite la factura, de todas formas la persona individual o jurídica paga el impuesto, pero el vendedor se apropia del mismo, debido a que no se origina la obligación para llevarla al fisco, lo que trae como consecuencia que se caiga en irregularidades y su consecuente sanción, de acuerdo con lo establecido en el Código Tributario.

f) Ley Orgánica del Instituto Guatemalteco de Seguridad Social y sus Reformas, Decreto número 295, establece los derechos y obligaciones entre el Patrono y el Empleado, regulando las fechas de pago, las cuotas laborales a retener y las cuotas patronales, así mismo, las suspensiones de los trabajadores por enfermedad común, accidentes, maternidad, programas de invalidez, vejes y sobrevivencia, entre otros.

g) Ley del Impuesto Sobre la Renta (ISR), Decreto número 26-92, establece un impuesto directo y que se genera cada vez que existan rentas grabadas por la empresa de calzado. Da a conocer en qué momento esta como persona jurídica actúa como contribuyente y como agente de retención.

h) Ley de Timbres Fiscales y de Papel Sellado Especial para Protocolos, Decreto número 37-92, genera un impuesto directo en el momento en que se realizan los pagos de dividendos efectuados a los accionistas de la empresa de calzado. La tarifa del impuesto es del 3% y se determina aplicándosela al valor de los dividendos pagados.

i) Ley del Impuesto Solidaridad (ISO), Decreto número 73-2008, afecta a las personas individuales o jurídicas que realicen actividades mercantiles o agropecuarias en el territorio nacional y obtengan un margen bruto superior al 4% de sus ingresos brutos.

j) Ley Sobre Productos Financieros, Decreto número 26-95, establece un impuesto especifico que grava los ingresos por intereses de cualquier naturaleza, incluyendo los provenientes de títulos-valores, públicos o privados, que se paguen en Guatemala, no sujetas a fiscalización de la Superintendencia de Bancos. El tipo impositivo es del 10% sobre la base definida anteriormente.

k) Disposiciones Legales para el Fortalecimiento de la Administración Tributaria, Decreto número 20-2006, el Organismo Ejecutivo busco el fortalecimiento de la Administración Tributaria, de una forma en que le permita ejercer un control más adecuado en las operaciones que realicen os contribuyentes debido a las prácticas de evasión y elusión provocadas por la debilidad, ambigüedad o carencia de normas precisas que permitan la generalidad, equidad y certeza del marco jurídico tributario.

Adicional a los aspectos mencionados previamente relacionados con otras leyes, el Decreto 20-2006 establece la creación del Registro Fiscal de Imprentas; un centro de autorización de facturas para cualquier entidad que preste servicios, también se crea la obligación a los contribuyentes que realicen pagos por montos mayores de Q 50,000.00 a utilizar el sistema bancario y no en efectivo.

CAPÍTULO II

LA AUDITORÍA DE SISTEMAS EN UNA INDUSTRIA DE CALZADO

2.1 ANTECEDENTES

En tiempos históricos, el auditor era aquella persona a quien se le leían los ingresos y gastos producidos por una empresa. (7:1)

Se estima que la primera auditoría nació desde el momento en que fue necesario rendir cuentas de un negocio y revisar que estas fueran correctas; fue evidente que dicha función fue evolucionando y simultáneamente crecimiento con la actividad de registros de las operaciones mercantiles.

Existe evidencia de que alguna especie de auditoría se practicó en tiempos remotos; el hecho que los empresarios exigieran el mantenimiento de las cuentas, pone de manifiesto que fueron tomadas algunas medidas para evitar desfalcos en dichas cuentas. A medida que se fue desarrollando el comercio, surgió la necesidad de las revisiones independientes para asegurar la conciliación y finalidad de los registros mantenidos en varias empresas. La auditoria como profesión, fue reconocida por primera vez bajo la Ley Británica de Sociedades Anónimas en 1862, que tuvo mandato sobre el sistema metódico y normalizado de contabilidad para una adecuada información para la prevención del fraude.

También reconoció una aceptación general de la necesidad de efectuar una versión independiente de las cuentas de las pequeñas y grandes empresas. Desde los años 1862 a 1905, la profesión de la auditoría creció y floreció en Inglaterra, posteriormente se introdujo a los Estados Unidos de Norte América y alrededor del mundo.

Al principio, la auditoria se consideró como una rama complementaria de la Contaduría Pública, y solo se dedicaba a examinar los registros contables y a la correcta presentación de los estados financieros de las empresas. Posteriormente, dicha aplicación se extendió a otros campos profesionales para ampliar su revisión; primero a los de carácter administrativo, después a los asociados a otras actividades de la empresa, luego se extendió a las ramas ingeniería, medicina, sistemas y así sucesivamente. (7:5)

La auditoria continúo desarrollándose no sólo respecto de fraudes, sino que también para revisar los estados financieros de las empresas y específicamente la posición financiera, a los resultados de operación, hasta concluir con la emisión de una opinión sobre tales estados. Conforme avanzó la tecnología, las condiciones imperantes requirieron que la auditoria se ampliara y se clasificara en varias ramas, surgiendo entonces la Auditoria en Sistemas.

En Guatemala, por medio del decreto gubernativo No. 1972 del 25 de mayo de 1937, aprobado en la Asamblea Legislativa, decreto No. 2270 del 19 de marzo de 1938, se crea la Facultad de Ciencias Económicas adscrita a la Universidad Nacional, dependiente del poder ejecutivo, así nace la profesión de Contador Público y Auditor.

Antes del año 1937, los Auditores en Guatemala eran de origen extranjero; sobresaliendo la señora Nancy de Lacy y el señor Joseph Gibson Davies, ambos de nacionalidad inglesa.

La única excepción guatemalteca fue el señor Joaquín Godoy que por razones de Estado recibió el título de Auditor, del General Lázaro Chacón, después de haber estudiado en los Estados Unidos de Norteamérica.

2.2 DEFINICIÓN

Auditoria. Es la revisión independiente que realiza un auditor profesional, aplicando técnicas, métodos y procedimientos especializados, a fin de evaluar el cumplimiento de funciones, actividades, tareas y procedimientos de una entidad administrativa, así como dictaminar sobre el resultado de dicha evaluación.

La auditoría se desarrolla como una actividad especializada que puede ejecutarse solo por quienes están capacitados profesionalmente para ello. Sin embargo es necesario que estos profesionales cuenten con los conocimientos, experiencias, actitudes y aptitudes necesarios para realizar este tipo de trabajo, a fin de cumplirlo tal y como demandan las empresas de la sociedad.

El resultado final de una auditoría es un informe de la misma, en donde el auditor, con absoluta libertad, profesionalismo y totalmente fundamentado en la aplicación de sus técnicas, herramientas y conocimientos de auditoría, informa sobre los resultados obtenidos durante su revisión.

El auditor tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo específico, que es el de evaluar la eficiencia y eficacia con que se está operando para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación. (5:2)

Auditoría interna. Es una actividad independiente, objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático, disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno. (16:1)

Informática. El concepto de informática es más amplio al simple uso de equipos de cómputo o bien de procesos electrónicos. La palabra Informática se deriva del francés informatique; este neologismo proviene de la conjunción de *information* (información) y automatique (automática).

En un concepto amplio, Informática es la ciencia del tratamiento sistemático y eficaz (realizado por medio de máquinas automáticas) de la información constituida como vehículo del saber humano y de la comunicación en los ámbitos técnico, económico y social.

Asimismo, se define como: La Ciencia de los sistemas inteligentes de información. (5:2-3)

Sistema. Un sistema es un conjunto de partes o elementos organizados y relacionados que interactúan entre sí para lograr un objetivo. Los sistemas reciben (entrada) datos, energía o materia del ambiente y proveen (salida) información, energía o materia.

Sistema informático. Es el conjunto de partes interrelacionadas, *hardware* (equipo), *software* (programas) y Recurso Humano. Un sistema informático típico utiliza una computadora que usa dispositivos programables para capturar, almacenar y procesar datos.

Auditoría Informática de sistemas. Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, *software* e información utilizados en una empresa, sean individuales, compartidos y/o redes así como sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. El propósito fundamental es evaluar el uso adecuado de la información y la emisión oportuna de sus resultados en la empresa, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de

funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa. (7:19)

Es una función que ha sido desarrollada para asegurar la salvaguarda de los activos de los sistemas de computadoras, mantener la integridad de los datos y lograr objetivos de la organización en forma eficaz y eficiente. (5:18)

Es la revisión y evaluación de los controles, sistemas y procedimientos de la informática; como también de los equipos de computo, su utilización, eficiencia y seguridad; de la organización que participa en el procesamiento de la información a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente, confiable y segura de la información tanto de los sistemas como de los equipos que servirá para una adecuada toma de decisiones. (5:18)

Este tipo de auditoría tiene como propósito evaluar la función de la tecnología de la información y de su aportación al cumplimiento de los objetivos organizacionales, con la finalidad de garantizar la seguridad de la información, planear el futuro, controlar el presente y evaluar el pasado, porque las operaciones de las empresas dependen cada vez mas de la sistematización por lo que tienden a aumentar los riesgos.

En síntesis, es un instrumento para asegurar el adecuado funcionamiento, protección y control de los elementos informáticos que contribuyen a proteger el patrimonio de la empresa y el logro de sus objetivos que es lograr la confiabilidad, oportunidad, seguridad de la información que se procesa a través de los sistemas de información, así mismo como los componentes físicos que lo integran.

¿Qué hace la auditoría informática?

- Detecta evidencia de riesgos y/o problemas en el apoyo informático a los procesos de negocios originados por mal manejo informático y/o control.
- Sugiere mejoras.

2.3 IMPORTANCIA

La informática está inmersa en la gestión integral de una empresa u organización. A finales del siglo XX, los sistemas de tecnologías de la información se constituyeron como las herramientas más poderosas para cualquier empresa, puesto que constituyen un valioso apoyo para la toma de decisiones, generando un alto grado de dependencia y una elevada inversión en ellas. Debido a la importancia que tienen en el funcionamiento de una empresa, existe la Auditoria Informática.

El término de auditoría ha sido utilizado con frecuencia de forma incompleta, porque solamente ha sido tomado como sinónimo de detección de errores y fallas; el concepto de auditoría es mucho más que eso, puesto que mediante el examen de sus políticas, sistemas y procedimientos relacionados con sus operaciones tiene también como fin evaluar, mejorar la eficiencia y eficacia de una empresa u organización.

Al igual que cualquier área de la organización, los sistemas de TI (tecnologías de la información) deben estar sometidos a controles de calidad y auditoría informática porque las computadoras y los centros de procesamiento de datos son blancos apetecibles para el espionaje, la delincuencia y el terrorismo. Al perder de vista la naturaleza y calidad de los datos de entrada a los sistemas de TI se genera información errónea, con la posibilidad de que se provoque un efecto cascada y afecte a otras aplicaciones. Asimismo, un sistema TI mal diseñado puede convertirse en una herramienta muy peligrosa para la gestión y la coordinación de la empresa.

Actualmente, la Auditoría Informática o sistemas es de vital importancia para el buen funcionamiento de los sistemas de proceso e información de la empresa, debido a que por su medio se incorporan los controles claves necesarios que permiten tener una seguridad razonable de que son confiables, oportunos y con un

buen nivel de funcionamiento y seguridad. En consecuencia, su ámbito de aplicación está dirigido a toda la estructura de la organización de las empresas, que invariablemente incluye a los centros de proceso de información, como a los equipos *(hardware)* y programas *(software)*.

2.3.1 Sus Beneficios

- Genera confianza en los usuarios sobre la seguridad y control de los servicios de TI.
- Optimiza las relaciones internas y el clima de trabajo.
- Disminuye los costos de la mala calidad (rechazos, reclamos, entre otros).
- Genera un balance de los riesgos en TI.
- Realiza un control de la inversión en un entorno de TI, a menudo impredecible.

2.4 OBJETIVOS GENERALES

Desde el punto de vista de un Departamento de Auditoría Interna, se establecen los siguientes objetivos de la Auditoría Informática: (11)

- Realizar una evaluación con personal suficientemente capacitado en el área de sistemas, con el fin de emitir un informe que indique sobre la razonable ejecución de las funciones del sistema y de la gestión administrativa del área de informática.
- Evaluar y analizar el uso de los recursos financieros en las áreas del centro de información y del aprovechamiento del sistema computacional, sus equipos periféricos e instalaciones.
- Evaluar el uso y aprovechamiento de los equipos de cómputo, sus periféricos, instalaciones y mobiliario del centro de cómputo, así como de sus recursos técnicos y materiales para el procesamiento de la información.

- Evaluar el aprovechamiento de los sistemas de procesamiento, sus sistemas operativos, lenguajes, programas y paquetes de aplicación y desarrollo e instalación de nuevos sistemas.
- Evaluar el cumplimiento de planes, programas, normas, políticas, y lineamientos que regulan las funciones y actividades de las áreas de trabajo y de los sistemas de procesamiento de información, así como del personal y de los usuarios del centro de información.

2.4.1 Objetivos para una buena gestión de los sistemas de la información en una empresa.

- Asegurar la mayor y mejor integridad, confidencialidad y confiabilidad de la información.
- Mantener la seguridad del personal, de los datos, equipos *(hardware)*, programas *(software)* e instalaciones.
- Eliminar o minimizar la existencia de riesgos en el uso de la tecnología de la información.
- Conocer la situación del área de informática para accionar al logro de los objetivos.
- Proveer seguridad, utilidad, confianza, privacidad y disponibilidad de los entornos.
- Incrementar la satisfacción de los usuarios de los sistemas informáticos.
- Capacitar y educar sobre los controles de los sistemas de información.
- Buscar mejorar la relación costo/beneficio de los sistemas automatizados.
- Tomar las mejores decisiones de inversión y eliminación de gastos innecesarios. (11)

2.5 FUNCIONES

Entre las funciones de los auditores informáticos de un Departamento de Auditoría Interna, se encuentra:

- Evaluar, verificar el control interno de las aplicaciones; de los sistemas tecnológicos y periféricos.
- Evaluar y Analizar la administración de los sistemas tecnológicos en cuanto a los riesgos de seguridad y de la efectividad de la administración.
- Analizar la gestión interna de los encargados de generar los sistemas de información.
- Analizar la integridad, fiabilidad y certeza de la información.
- Evaluar los riesgos operativos de los circuitos de información.
- Analizar la gestión interna e los encargados de medir los riesgos de la información.
- Verificar el nivel de continuidad de los sistemas y procedimientos.
- Analizar el estado del arte tecnológico de la instalación revisada.
- Diagnosticar sobre el grado de cobertura de las aplicaciones a las necesidades estratégicas y operativas de la información de la empresa.
- Establecer los objetivos de control y emitir las recomendaciones de control que eliminen o minimicen la exposición al riesgo de control interno.

2.6 ELEMENTOS

Los siguientes elementos informáticos son definidos para propósitos de realizar una Auditoría Informática: (14:1)

- El Desarrollo de Sistemas.
- Las Bases de Datos.
- La calidad del proceso, registro y generación de la información.
- La instalación y funcionamiento de los sistemas operativos.

- La consecución de la Ofimática.
- La instalación y funcionamiento de redes.

2.6.1 Auditoria Desarrollo de Sistemas

El objetivo primario de esta auditoría es el de evaluar la suficiencia y eficacia de los controles internos. El objetivo de la función de los diseñadores de sistemas consiste en satisfacer las necesidades de los usuarios. Por lo consiguiente, los encargados deben compartir el deseo de asegurar el logro de cada objetivo.

La auditoría asegura que los controles hayan sido bien establecidos y que estén siendo aplicados y funcionando apropiadamente; asimismo, porque los sistemas recientemente implantados incluyan características de control sólidas y confiables. En general, este tipo de auditoría ayuda a que se implanten apropiados sistemas computarizados que permitan eliminar o reducir los riesgos de fallas, debilidades importantes que podrían tener efectos negativos y adversos en la operación de las empresas.

La auditoría necesita reconocer que su participación durante el desarrollo de los sistemas puede amenazar su independencia y deberá tomar medidas para evitar esta pérdida. Estas medidas incluyen: (14:8)

- Permanecer organizacionalmente independiente del grupo de sistemas. Significa que la auditoría no es un miembro en propiedad del grupo de desarrollo de sistemas y no le quita la dirección del proyecto al gerente del grupo del proyecto.
- Investigar independientemente del grupo del proyecto. El grupo del proyecto puede estar restringido a ciertos contactos y cierta autoridad, pero la auditoría tiene libre acceso a la información y al personal de la organización.

El área de desarrollo, y la auditoría, son importantes para las empresas por las siguientes razones: a) Los avances en tecnología de informática ha hecho que el principal factor de éxito sea el de mejorar la calidad de los equipos (*hardware*) y programas (*software*), b) Los fondos destinados a la adquisición de equipos y programas es cada vez mayor, c) Los programas (*software*) como producto es muy difícil de validar (a mayor control, mejor calidad y menores costos de mantenimiento), d) El índice de fracasos en proyectos de desarrollo es muy alto, y, d) Los sistemas computarizados constituyen una valiosa herramienta de trabajo esencial para la administración en la toma de decisiones.

2.6.2 Auditoría de Bases de Datos

Es el proceso que permite medir, asegurar, demostrar, monitorear y registrar los accesos a la información almacenada en la base de datos, incluyendo la capacidad de determinar: (14:10)

- ✓ Quién accede a los datos
- ✓ Cuando se accedió a los datos
- ✓ Desde que tipo de dispositivo o aplicación
- ✓ Desde que ubicación en la red
- ✓ Cual fue el efecto del acceso a la base de datos

2.6.3 Auditoría a la Calidad

Se utiliza como una valiosa herramienta de gestión para verificar y evaluar las actividades relacionadas con la calidad en el seno de una empresa u organización. Su realización se inicia en una o varias de las siguientes situaciones: (14:4)

Por solicitud de la Administración. La administración está facultada para someter a auditoría el sistema de gestión de la calidad de un centro de fabricación como una medida más dentro del proceso de verificación de un producto.

Por solicitud a una entidad de certificación. (14:4) Una organización puede solicitar la certificación de que su sistema de calidad es conforme al modelo adoptado y, en consecuencia, someterse a una auditoría.

La auditoría puede ser el fruto del propio sistema de calidad de la organización, o bien obedecer a pautas ajenas en manos de terceros, sea del ente de certificación de un cliente o de la propia Administración. En cualquiera de los casos, la alta dirección debe disponer de los medios más adecuados para su realización, así como para la identificación y mejora de las áreas no conformes al modelo exigido.

Por ello, es responsabilidad de la Gerencia y alta dirección establecer un programa de Auditorías Interna,s verificar su adecuada implementación y funcionamiento. Desarrollar un programa de auditorías puede entenderse como satisfacer las exigencias de un determinado cliente o entidad.

Las auditorías de calidad proporcionan a la alta dirección de la empresa, evidencias objetivas lo cual le permitirá tomar decisiones acertadas (auditorías basadas en hechos y no en hipótesis).

2.6.4 Auditoría de sistemas operativos

Consiste en revisar las políticas y procedimientos de adquisición y mantenimiento de *software* de sistemas operativos como también el *hardware*. Para lo cual la auditoría revisa lo siguiente:

Los procedimientos relacionados con la identificación y la selección del *software* del sistema y el *hardware*. Mediante entrevistas a la gerencia, para identificar:

- Los requerimientos de *software y hardware*.
- Las fuentes potenciales de *software y hardware*.

Análisis de costo/beneficio del *software* y *hardware*. Consiste en revisar la documentación del análisis costo/beneficio y las alternativas que proponen y determinan si cada alternativa potencial fue evaluada adecuadamente. Esta documentación debe tener por lo menos:

- Costo directo financiado para la compra de *software* y del equipo que será utilizado para la implementación del sistema.
- Costo de la modificación necesaria para adaptar el *software* al ambiente de sistemas de información de la organización (si fuera necesario) como también el *hardware*.
- Los requisitos de equipo para ese *software*.
- Los requisitos de capacitación asociados con la utilización de ese *software*.
- Los requisitos de apoyo técnico asociado a ese software.
- Análisis de las facilidades del software para cumplir con los requisitos de procesamiento de información.
- Análisis de la capacidad del software para cumplir con los requisitos de seguridad.
- Análisis de la capacidad del software para cumplir con los requisitos técnicos de la organización.

Instalación del software del sistema. Consiste en revisar el plan o procedimiento para la prueba del sistema, determinar si las pruebas se realizaron de acuerdo a ese plan y en forma exitosa, de no ser así investigar si todos los problemas se evaluaron y resolvieron antes de la instalación del *software*. También es muy

importante verificar la instalación del *software* al equipo si se encuentra en buenas condiciones si llena el perfil adecuado para buen funcionamiento del *software*.

Mantenimiento del *software* del sistema. Consiste en revisar la documentación relacionada con el mantenimiento del *software* y determinar lo siguiente:

- Si los estándares de instalación están de acuerdo con la documentación del mantenimiento del *software*.
- Si los cambios en el *software* del sistema están debidamente explicados en cuanto a su motivo y aprobación.
- Si existen pruebas de que el cambio realmente se hizo.
- Si el personal responsable del cambio del *software* del sistema no pertenece al grupo de programadores.
- Si se proporciona a los usuarios del sistema documentación sobre los cambios que se realizarán.
- Si existe un registro o una bitácora de los cambios realizados al sistema.
- Si existen los controles suficientes para asegurarse que los operadores no podrán hacer cambios al sistema sin asesoría del grupo responsable de la instalación de estos cambios.

Seguridad del *software* del sistema. Consiste en revisar los procedimientos para el acceso al *software* del sistema y a su documentación, para esto entrevistarse con la gerencia o con el personal adecuado para identificar los procedimientos de seguridad para restringir el acceso al *software* del sistema así como el personal que tiene acceso al *software* del sistema y a su documentación.

Seguridad del *hardware*. Consiste en revisar los procedimientos, políticas con las que cuenta la empresa en la compra/venta, las reparaciones, mantenimientos que se les efectúen a los equipos, como verificar si tienen contrato de a seguranza por alguna catástrofe que surja, la ubicación del equipo, así como el personal que esté a cargo de los equipos.

2.6.5 Auditoría a la ofimática

La Ofimática se refiere a los programas o aplicaciones que en conjunto sirven de herramienta para generar, procesar, almacenar, recuperar, comunicar y presentar la información en un lugar de trabajo. (14:5)

El programa *(software)* de Ofimática comprende una serie de aplicaciones que se distribuyen de forma conjunta para ser empleadas simultáneamente en diversos sistemas.

Usualmente, las herramientas de Ofimática se refieren a:

- Aplicaciones de productividad personal
- Administradores de Bases de Datos
- Hojas de cálculo
- Procesadores de Textos
- Presentadores de ideas
- Gráficos

Existen dos características al analizar en el entorno de Ofimática: a) La distribución de las aplicaciones por los diferentes departamentos de la empresa u organización en lugar de centralizarse en una única ubicación, y, b) El traslado de la responsabilidad sobre ciertos controles de los sistemas de información a usuarios finales no dedicados profesionalmente a la informática, quienes pueden no comprender de un modo adecuado la importancia de éstos y la forma de realizarlos.

Los controles básicos de auditoría pueden también aplicarse en este entorno y se constituyen como muy importantes para la empresa u organización, ya que están referidos a los siguientes conceptos:

Economía, eficiencia y eficacia.

A continuación presenta lo siguiente:

1. Determinar si el inventario Ofimático refleja con exactitud los equipos y aplicaciones existentes en la empresa u organización.
2. Determinar la propiedad de los procedimientos de adquisiciones de equipos y aplicaciones.
3. Determinar y evaluar la propiedad de la política de mantenimiento definida en la empresa u organización.
4. Determinar si la calidad de las aplicaciones del entorno Ofimático desarrollada por el personal de la empresa u organización, es aceptable.
5. Evaluar la necesidad de corrección del procedimiento existente en cuanto a los cambios de versiones y aplicaciones.
6. Determinar si los usuarios cuentan con la suficiente formación y la documentación de apoyo necesaria para desarrollar sus tareas de un modo eficaz y eficiente.
7. Determinar si el sistema se ajusta a las necesidades reales de la empresa u organización.

Seguridad

A continuación presenta lo siguiente:

1. Determinar si la empresa cuenta con garantías suficientes para proteger los accesos no autorizados a la información reservada y la integridad de la misma.
2. Determinar si el proceso de generación de copias de respaldo es confiable y garantiza la recuperación inmediata de información en caso de necesidad.
3. Determinar si está garantizado el funcionamiento interrumpido de aquellas aplicaciones, cuya caída podría suponer pérdidas importantes de la integridad de la información y aplicaciones.

4. Determinar el grado de exposición ante la posibilidad de contagio de virus y las medidas preventivas existentes.

2.6.6 Auditoría de Redes

Los sistemas de comunicación, desde el punto de vista de auditoría, presentan problemas comunes debido a que la información transita por lugares físicamente alejados de las personas responsables. Esto presupone un compromiso en seguridad, porque no existen procedimientos físicos que garanticen la inviolabilidad de la información.

En las redes, por causas propias de la tecnología, puede producirse básicamente tres tipos de incidencias: a) Alteración de bits, b) Ausencia de tramas, y, c) Alteración de la secuencia.

Los tres mayores riesgos a controlar son: a) La indagación (casos en que un tercero puede leer la información), b) Suplantación (casos en que un tercero introduce un mensaje falso que el receptor cree proviene del emisor legítimo), y, c) Modificación (casos en que un tercero altera el contenido de un mensaje).

El primer punto de una auditoría de comunicaciones, consiste en determinar que la función de administración de redes y comunicaciones está claramente definida, y que entre otros, exista: a) Una gerencia de comunicaciones con autoridad para establecer procedimientos y políticas, b) Procedimientos, registros de inventario y cambios, c) Funciones de vigilancia, uso de la red, ajustes a rendimientos, registro de incidencias y resolución de problemas, d) Procedimientos para el seguimiento al costo de las comunicaciones y su adecuada distribución a las áreas correctas, e) Monitoreo del uso de la red para realizar mejoras en rendimiento, f) Planes de comunicación de corto y largo plazo, incluyendo estrategias de comunicaciones de voz y de datos, g) Normas para el tipo de equipo que puede ser instalado en la red, y, h) Procedimientos de autorización para conectar nuevos equipos a la red.

En la auditoría de la red física es importante: a) Analizar las garantías que ofrecen las instalaciones físicas de los edificios, b) Si han sido estudiadas y evaluadas las probables vulnerabilidades existentes, c) Comprobar el hecho que los accesos físicos desde el exterior han sido registrados y que desde el interior del edificio no se intercepta físicamente el cableado, d) Analizar y probar las acciones preventivas que permitan establecer oportunamente cual es la parte del cableado que puede continuar funcionando y hasta que actividad puede soportar en caso de siniestros.

Algunos de los objetivos de control de esta importante área de la organización, que constituyen acciones preventivas para eliminar o reducir los casos de accesos no autorizados, son los siguientes: a) Registro y seguimiento a los equipos de comunicaciones, b) Protección, tendido adecuado de cables y líneas de comunicaciones, c) Monitoreo de la red y su tráfico, registros de su utilización, y, d) Registros específicos en casos de utilización de líneas telefónicas con acceso a red de datos.

En el aspecto lógico, es necesario monitorear la red, analizar los errores que se producen estableciendo procedimientos para detectar y aislar equipos que presenten comportamientos inadecuados. Como objetivos de control, se presentan: a) Marcar la existencia de contraseñas y otros procedimientos para limitar y detectar cualquier intento no autorizado a la red, b) Establecer facilidades para la detección de errores de transmisión y retransmisiones apropiadas, c) Asegurar que las transmisiones se dirigen solamente a usuarios autorizados, d) Registrar la actividad de la red para ayudar a reconstruir incidencias, eliminar y detener accesos no autorizados, e) Incorporar técnicas de cifrado de datos en donde se establezca que existe riesgo de accesos no autorizados a transmisiones confidenciales, y, f) Realizar pruebas periódicas en que se simulen ataques para descubrir vulnerabilidades, documentando los resultados y corrigiendo las deficiencias encontradas. (14:11)

2.7 REFERENCIAS TÉCNICAS PARA LA PRÁCTICA DE LA AUDITORÍA INTERNA.

Los estándares profesionales que sirven de referencia para el desarrollo del trabajo de la Auditoría Interna, son: Las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna las cuales fueron emitidas por el Instituto de Auditores Internos (*THEIIA*), sus siglas en inglés.

El propósito de las Normas es:

1. Definir principios básicos que representen el ejercicio de la auditoria interna tal como este debería ser.
2. Proveer un marco para ejercer y promover un amplio rango de actividades de auditoría interna de valor añadido.
3. Fomentar la mejora en los procesos y operaciones de la organización. (16:1)

- **Normas Sobre Desempeño**

2100 Naturaleza del trabajo: Establece que los Auditores Internos deben considerar mejorar los controles relacionados con los riesgos de las actividades de la organización. Se subdivide en:

2110 Gestión de riesgos: Esta trata sobre la identificación y evaluación de riesgos significativos para la organización y en su párrafo A2 estipula: "Que la actividad de auditoría interna debe evaluar las exposiciones al riesgo referidas a gobierno, operaciones y sistemas de información de la organización, con relación a lo siguiente:

- Confiabilidad e integridad de la información financiera y operativa.
- Eficacia y eficiencia de las operaciones,
- Protección de activos y
- Cumplimiento de leyes, regulaciones y contratos." (16:8)

2120 Control: La actividad de auditoría interna debe asistir a la organización en el mantenimiento de controles efectivos, mediante la evaluación y eficiencia de los mismos y promoviendo la mejora continúa. En el párrafo A1 se basa en los resultados de la evaluación de riesgos, la actividad de auditoría interna debe evaluar la adecuación y eficiencia de los controles que comprenden el gobierno, las operaciones y los sistemas de información de la organización.

CAPÍTULO III

EL CONTROL INTERNO INFORMÁTICO SOBRE LA SEGURIDAD DEL ÁREA DE SISTEMAS

3.1 ANTECEDENTES

El origen del Control Interno, suele ubicarse en el tiempo con el surgimiento de la partida doble, considerada como una de las medidas de control, pero no fue sino hasta fines del siglo XIX que los hombres de negocios se preocuparon por formar y establecer sistemas adecuados para la protección de sus intereses.

A finales de ese siglo, como consecuencia del aumento de la producción, los propietarios de los negocios imposibilitados de continuar atendiendo personalmente los problemas productivos, comerciales y administrativos, se vieron forzados a delegar funciones dentro de la organización y a promover la creación de sistemas y procedimientos que previnieran o disminuyeran los casos de fraude o errores. Debido a esto, se sintió entonces la necesidad de incorporar controles sobre la gestión de los negocios, ya que en realidad se había prestado más atención a la fase de producción y comercialización que a la administrativa u organizativa, reconociéndose así la necesidad de crear e implementar Sistemas de Control.

Los contadores idearon la "comprobación interna" para asegurarse contra posibles errores y fraudes. "La comprobación interna es el término con el que se llamaba a lo que es hoy Control Interno, que era conocida como la organización y coordinación del sistema de contabilidad y los procedimientos. (15)

El Control Interno ha venido evolucionando al grado tal que actualmente es de vital importancia aplicarlo en las empresas u organizaciones. Los empresarios y administradores ya tienen bastante claro que sin esta valiosa herramienta de gestión y control, los riesgos de ineficacia e inoperancia están latentes.

Definición

El Control Interno comprende el plan de organización, los métodos y procedimientos que en forma coordinada se adoptan en un negocio para salvaguardar sus activos, verificar la exactitud y confiabilidad de la información financiera, proveer la eficiencia operativa y provocar la adherencia a las políticas prescritas por la administración. (7:97)

Importancia

El Control Interno, reviste vital y singular importancia en las empresas, tanto porque contribuye en la conducción de su organización, como por el impulso al apropiado, oportuno registro de operaciones y la emisión de la información correspondiente. También porque apoya y obliga al manejo adecuado de los activos y al eficiente desempeño de las funciones del personal. El fin primordial es el de generar una indicación confiable de su efectividad y de la eficacia de las operaciones en el mercado; asimismo, a que los recursos disponibles (humanos, materiales y financieros) sean aplicados y utilizados en forma eficiente, bajo criterios técnicos que permiten asegurar los conceptos, aplicaciones de integridad, custodia y registro oportuno. La importancia del Control Interno para las empresas, radica en que: (7:106)

- Permite controlar eficazmente las operaciones; la administración necesita de la precisión de numerosos informes y análisis relacionados.
- Contribuye a la salvaguarda de los activos; previene y detecta oportunamente errores y fraudes.

- Funciona en contra de las debilidades humanas; debido a que elimina o reduce la posibilidad de que errores o intentos fraudulentos queden sin ser descubiertos por un periodo prolongado y porque permite a la administración depositar mayor confianza en la veracidad de los datos.

3.2 OBJETIVOS DEL CONTROL INTERNO

- Proteger los activos: Custodia apropiada; asegura la salvaguarda e incorpora medidas de prevención para el uso no autorizado y disposición ilegal. Este involucra: a) Niveles de Autorización, tendiente a que todas las operaciones se realicen de acuerdo con las autorizaciones generales o especificas de la administración y, b) La Salvaguarda Física en cuanto a que el acceso a los activos solo debe permitirse a aquellos que cuenten con las autorizaciones de la administración.

- Asegurar registros contables correctos y exactos: Captura y procesamiento de datos en forma completa y exacta.

- Fomentar la eficiencia operacional: Ejecutar operaciones de acuerdo con apropiados niveles de autorización en función de criterios aprobados y establecidos por la administración; aceptar solo procesos oportunos y transacciones autorizadas.
- Estimular el cumplimiento oportuno de las políticas: Aplicar en la práctica, las políticas aprobadas por la Administración y los lineamientos que incluyen; asimismo, aplicar la consistencia de políticas de un año a otro.
- Contar con métodos y registros: Aquellos que identifiquen y registren únicamente las transacciones reales reuniendo los criterios establecidos por la administración.

- Implementar métodos, técnicas y procedimientos: Los cuales permitan desarrollar adecuadamente las actividades, tareas y funciones de la empresa. (7:107)

3.3 PRINCIPIOS DEL CONTROL INTERNO

El control interno implica la aplicación de los principios de igualdad, moralidad, eficiencia, economía, celeridad, imparcialidad, publicidad y valoración de costos ambientales.

- El principio de igualdad consiste en velar porque las actividades de la empresa estén orientadas hacia el interés general, sin otorgar privilegios a grupos especiales.
- El principio de moralidad enfatiza a que todas las operaciones sean realizadas acatando las normas aplicables a la empresa y los principios éticos y morales que rigen la sociedad.
- El principio de eficiencia vela por la igualdad de condiciones de calidad y oportunidad, la provisión de bienes y/o servicios al mínimo costo con la máxima eficiencia y el mejor uso de los recursos disponibles.
- El principio de economía vigila porque la asignación de recursos sea la más adecuada en función de los objetivos y las metas de la empresa.
- El principio de celeridad consiste en la capacidad de la empresa en dar respuesta oportuna a las necesidades del ámbito de su competencia.
- Los principios de imparcialidad y publicidad están dirigidos a obtener la máxima transparencia en las actuaciones de la empresa, de tal manera que no exista alguna persona o entidad que sea afectado en sus intereses u objeto de discriminación, tanto en oportunidades como en el libre acceso a la información.

- Como un factor importante en la toma de decisiones y en la conducción de las actividades rutinarias en aquellas empresas en las cuales su operación pueda tenerlo, el principio de valoración de costos ambientales pretende la reducción al mínimo del impacto ambiental negativo.

Un Control Interno eficiente, presupone necesariamente la existencia de objetivos y metas en la organización, si estos no están bien definidos, la organización carecerá de rumbo y por lo tanto, de un marco referente contra el cual pueda medir los resultados obtenidos.

3.4 FINALIDAD DEL CONTROL INTERNO.

El deterioro del patrimonio no proviene solo de la ilegalidad de una inversión, también se deriva de su inconveniencia. Así la falta de planeación o programación, en muchos casos, puede producir gastos inútiles, aunque sean legales.

El control interno no debe limitarse a vigilar la legalidad y exactitud de las operaciones, sino que también a buscar un fin más amplio, adecuado a los cambios administrativos, presupuestales, operativos y financieros. En tal sentido, incluye analizar la utilidad de la inversión y la obtención de los resultados previstos.

El auditor estudia y evalúa el sistema de Control Interno para obtener una seguridad razonable de que se alcanzan los objetivos previstos. Utiliza pruebas de cumplimiento para obtener certeza razonable de que los procedimientos de control interno se estén aplicando en la forma prevista y asume la responsabilidad de informar las deficiencias encontradas principalmente las recomendaciones para propósitos de mejora.

3.5 CONTROL INTERNO DE ACUERDO A COSO ERM

El Comité de las Organizaciones Patrocinadoras de la Comisión de Treadway (COSO), el cual se define como un proceso que garantice una seguridad razonable (y por lo tanto no absoluta), que se alcanzan los tres objetivos siguientes:

Efectividad y eficiencia de las operaciones:
Trata los objetivos de negocio básicos de una entidad, incluyendo metas del funcionamiento, de lo beneficioso y salvaguarda de recursos.

Confiabilidad de la Información financiera y administrativa:
Se relaciona con la preparación de estados financieros confiables, incluyendo estados financieros provisionales o condensados, así como datos financieros seleccionados derivados de tales declaraciones.

Observancia de las leyes y regulaciones aplicables:
Se ocupa de las disposiciones legales y regulatorias.

Se puede decir que el control interno es todo, incluye toda la organización, los mecanismos, métodos, medidas que se diseñan, implantan y mantienen para asegurar que se logren los objetivos, que se cumpla con las funciones, tareas relacionadas con la previsión, seguimiento y control de las actividades económicas, financieras y administrativas.

Es la gestión de riesgos empresariales el cual se efectúa por el consejo administrativo de la entidad, su dirección y restante personal, que se aplica a la definición de estrategias en toda la empresa y diseñado para identificar eventos potenciales que puedan afectar la organización, gestionar sus riesgos dentro del riesgo aceptado y proporcionar seguridad razonable sobre el logro de objetivos.

Esta definición recoge los siguientes conceptos básicos de la gestión de riesgos empresariales:

- Es un proceso continuo que fluye por toda la entidad.
- Es realizado por su personal en todos los niveles de la organización.
- Se aplica en el establecimiento de la estrategia.
- Se aplica en toda la entidad, en cada nivel y unidad, e incluye adoptar una perspectiva del riesgo a nivel conjunto de la entidad.
- Está diseñado para identificar acontecimientos potenciales que, de ocurrir, afectarían a la entidad y para gestionar los riesgos dentro del nivel aceptado.
- Es capaz de proporcionar una seguridad razonable al consejo de administración y a la dirección de una entidad.

La base fundamental en la gestión de riesgos empresariales (ERM), es que las entidades existen con el fin último de generar valor para sus grupos de interés. Todas se enfrentan a la ausencia de certeza y el reto para su dirección es determinar cuanta incertidumbre se puede aceptar mientras se esfuerzan en incrementar el valor para sus grupos de interés.

La incertidumbre implica riesgos y oportunidades que posee el potencial de erosionar o aumentar el valor. La gestión de riesgos empresariales permite a la dirección tratar eficazmente la incertidumbre, sus riesgos y oportunidades asociados, mejorando así la capacidad de generar valor.

La gestión de riesgos empresariales nos ayuda a la dirección a alcanzar los objetivos de rendimiento, la rentabilidad de la entidad, prevenir pérdida de recursos, asegurar una información eficaz y el cumplimiento de leyes y normas, además de ayudar a evitar daños a la reputación de la entidad y sus consecuencias derivadas. En suma, la gestión de riesgos empresariales ayuda a una entidad a llegar al destino deseado, evitando baches y sorpresas por el camino.

3.6 COMPONENTES DEL CONTROL INTERNO COSO ERM

El marco integrado de control que plantea el COSO-ERM (Gestión del Riesgo Empresarial) consta de ocho componentes interrelacionados, derivados del estilo de la dirección, e integrados al proceso de gestión, siendo los siguientes: (4:7)

1. Ambiente interno.
2. Establecimiento de objetivos.
3. Identificación de eventos.
4. Evaluación de Riesgos.
5. Respuesta al Riesgo.
6. Actividades de Control.
7. Información y comunicación.
8. Supervisión.

El ambiente interno refleja el espíritu ético vigente en una entidad respecto del comportamiento de los agentes, la responsabilidad con que encaran sus actividades, y la importancia que le asigne el control interno.

Sirve de base de los otros componentes, ya que es dentro del ambiente que se evalúan los riesgos y se definen las actividades de control tendientes a neutralizarlos. Juntamente se capta la información relevante y se realizan las comunicaciones pertinentes, dentro de un proceso supervisado y corregido de acuerdo con las circunstancias.

Este modelo refleja el propio dinamismo de los sistemas de control interno. Así también la evaluación de riesgos no solo influye en las actividades de control, sino que puede también poner de relieve la conveniencia de reconsiderar el manejo de la información y la comunicación.

Existe una relación directa entre los objetivos (Eficiencia de las operaciones, confiabilidad de la información y cumplimiento de leyes y reglamentos) y los ocho componentes referenciados, la que manifiesta permanentemente en el campo de la gestión: las unidades operativas y cada agente de la organización conforman secuencialmente un esquema orientado a los resultados que se buscan, y la matriz constituida por ese esquema es a su vez cruzada por los componentes.

3.6.1 Ambiente Interno

El conjunto de circunstancias que enmarcan el funcionamiento de una empresa desde la perspectiva del Control Interno y que son determinantes por el grado en que los principios de este último imperan sobre las conductas y los procedimientos organizacionales. Es fundamental la actitud de la alta dirección y de la gerencia, y por ende de los demás agentes con relación a la importancia del Control Interno y su incidencia sobre las actividades y resultados. (4:21)

El ambiente de control fija el entorno de la organización, y sobre todo, provee disciplina por la influencia que ejerce sobre el comportamiento del personal en su conjunto.

Constituye la base para el desarrollo de las acciones, y por ello su trascendencia, pues como conjunción de medios, operadores y reglas previamente definidas, traduce la influencia colectiva de varios factores en el establecimiento, fortalecimiento o debilitamiento de las políticas y procedimientos efectivos en una organización.

Se consideran los principales factores del Ambiente Interno:

- La filosofía y estilo de la Dirección y la Gerencia.
- La estructura, el plan organizacional, los reglamentos y los manuales de procedimientos.

- La integridad, los valores éticos, la competencia profesional, el compromiso de todos los participantes, componentes de la organización, así como su adhesión a las políticas y objetivos establecidos.
- Las formas de asignación de responsabilidades y de la administración y desarrollo del personal.
- El grado de documentación de políticas y decisiones, y de formulación de programas que contengan metas, objetivos e indicadores de rendimiento.

El Ambiente de Control será tan bueno, regular o malo, como lo sean los factores que lo determinan. El mayor o menor grado de desarrollo y excelencia de estos factores, originará en ese mismo orden, la fortaleza o debilidad del ambiente y consecuentemente el entorno de la organización. (12)

3.6.2 Establecimiento de objetivos

Dentro del contexto de misión o visión de una entidad, la dirección establece los objetivos, selecciona la estrategia y fija los objetivos alineados que fluyen en cascada en toda la entidad. Este marco de gestión de riesgos empresariales está orientado a alcanzar los objetivos de la empresa, que pueden clasificarse en cuatro categorías:

1. Estrategia: objetivos a alto nivel, alineados con la misión de la entidad y con el apoyo necesario.
2. Operaciones: objetivos vinculados al uso eficaz y eficiente de los recursos.
3. Información: objetivos de confiabilidad de la información y datos suministrados.
4. Cumplimiento: objetivos relacionados al cumplimiento de leyes y normas aplicables.

Esta clasificación de objetivos permite enfocarse en aspectos diferenciados de la gestión de riesgos empresariales, dirigidos a las necesidades que puedan surgir y de responsabilidad directa de diferentes ejecutivos. (12)

3.6.3 Identificación de Eventos

Se identifican eventos potenciales en todos los niveles de la organización de las empresas, que de ocurrir, pueden afectarla adversamente. Usualmente, estos eventos son originados por acontecimientos internos o externos con efectos e impactos negativos, positivos o de ambos.

Los eventos internos o externos con efectos e impacto negativo representan altos riesgos, de hasta incluso impedir el logro de los objetivos establecidos por las administraciones de las empresas o bien erosionar el valor existente.

Los eventos internos o externos con efectos e impacto positivo representan oportunidades que derivan la posibilidad de que contribuyan al logro de los objetivos, ayudando a la creación de valor o a su conservación. (4:28)

3.6.4 Evaluación de Riesgos

El control interno ha sido desarrollo esencialmente para eliminar o limitar los riesgos a que están afectas las actividades de las empresas. A través de la investigación y análisis de los riesgos relevantes y del punto hasta el cual el control vigente los neutraliza, se evalúa la vulnerabilidad del sistema. Se adquiere un conocimiento práctico de la entidad y de sus componentes de manera tal que se identifican los puntos débiles, enfocando los riesgos tanto internos como externos.
El establecimiento de objetivos es precedente a la evaluación de riesgos. Si bien los objetivos no constituyen un componente del Control Interno, si constituyen un requisito previo para el funcionamiento de este.

Los objetivos relacionados con las operaciones y con la información financiera pueden ser implícitos o explícitos, y generales o particulares. Con el establecimiento de objetivos globales y por actividad, una empresa puede identificar los factores críticos del éxito y determinar los criterios para medir el rendimiento.

Los objetivos de control deben ser específicos, adecuados, completos, razonables e integrados a los objetivos globales de la institución. El análisis de riesgos incluye:

- Una estimación de su importancia/trascendencia.
- Una evaluación de la probabilidad/frecuencia.
- Una definición del modo en que habrá de administrarse.

Otras circunstancias merecen atención especial en función del impacto potencial que plantean; por ejemplo:

- Los cambios en el entorno.
- La redefinición de la política institucional.
- Las re-organizaciones o re-estructuraciones internas.
- El Ingreso de nuevos empleados o la rotación de los existentes.
- Los nuevos sistemas, procedimientos y tecnologías.
- La aceleración del crecimiento.
- Los nuevos productos, actividades o funciones.

3.6.5 Respuesta al Riesgo

La Dirección de cada empresa, selecciona las posibles respuestas para eliminar, evitar, aceptar, reducir o compartir los riesgos, desarrollando una serie de acciones, definiendo las tolerancias permisibles.

El Director de Riesgos, Director Financiero, Auditor Interno u otros, desempeñan responsabilidades claves. El personal restante de la entidad es responsable de ejecutar la gestión de riesgos empresariales de acuerdo con las directrices y protocolos establecidos.

El Consejo Administrativo desarrolla una importante supervisión de la gestión de riesgos empresariales que es consciente del riesgo aceptado y está de acuerdo con el mismo.

Algunos terceros, como por ejemplo clientes, proveedores, colaboradores, auditores externos, y analistas financieros, proporcionan información útil para el desarrollo de la gestión de riesgos empresariales, aunque no son responsables de su eficacia. (12)

3.6.6 Actividades de Control

Están basadas en procedimientos específicos establecidos como un re-aseguro para el cumplimiento de los objetivos y orientados primordialmente hacia la prevención y neutralización de los riesgos.

Las actividades de control se ejecutan en todos los niveles de la empresa y también en cada una de las etapas de la gestión. Conociendo los niveles de riesgo, se dispone de controles dirigidos a su eliminación o reducción. Según el objetivo de la entidad con el que estén relacionados, estos controles se agrupan en tres categorías de: (4:37)

- Las operaciones
- La confiabilidad de la información financiera
- El cumplimiento de leyes y reglamentos.

La amplitud de alcance de las actividades de control comprenden a muchos asuntos importantes, los más conocidos y de usual aplicación se refieren a:

- Los análisis de la Dirección.
- El seguimiento y revisión por los responsables de las diversas actividades.
- La comprobación de las transacciones en cuanto a exactitud, totalidad, y autorización pertinente (aprobaciones, revisiones, cotejos, re-cálculos, análisis de consistencia, pre-numeraciones).
- Los controles físicos patrimoniales, arqueos, conciliaciones, re-cuentos.
- Los dispositivos de seguridad para restringir el acceso a los activos y registros.
- Una apropiada segregación de funciones.
- La aplicación de indicadores de rendimiento.

Es importante contar con apropiados controles de las tecnologías de la información, pues estas desempeñan un papel fundamental en la gestión, destacándose el centro de procesamiento de datos, la adquisición, implantación y mantenimiento de los programas (software), la seguridad en el acceso a los sistemas, los proyectos de desarrollo y el mantenimiento de las aplicaciones.

3.6.7 Información y Comunicación

Todos los agentes deben conocer la función que les corresponde desempeñar en la organización (deberes, funciones y responsabilidades). En tal sentido, es importante que cuenten con la información periódica y oportuna que les permita orientar sus acciones en coordinación con los demás hacia el cumplimiento de los objetivos. Es vital que la información sea captada, procesada y transmitida de tal modo que llegue oportunamente a todos los sectores permitiendo asumir las responsabilidades individuales que corresponda.

Los sistemas de información permiten identificar, recoger, procesar y divulgar datos relativos a los hechos o actividades internas y externas, funcionando muchas veces como herramientas de supervisión a través de rutinas previstas para tal efecto. No obstante resulta importante mantener un esquema de información acorde a las necesidades de la empresa, que en un contexto de cambios constantes, evoluciona rápidamente.

La comunicación es un aspecto inherente a los sistemas de información. El personal debe conocer sus responsabilidades de gestión en forma oportuna. Cada función debe diseñarse y comunicarse con oportunidad y claridad, bajo un entendimiento apropiado de los aspectos relativos a la responsabilidad de los individuos dentro del sistema de Control Interno.

El personal debe conocer con amplitud como están relacionadas sus actividades con el trabajo de los demás, los comportamientos esperados y la manera de comunicar la información relevante que generen.

Los informes deben transferirse adecuadamente a través de una comunicación efectiva y eficaz. (12)

3.6.8 Supervisión

Consiste en la revisión y actualización periódica, vigilante de las actuaciones y resultados, que permite mantener un nivel adecuado para la evaluación de las actividades de control de los sistemas.

El objetivo de la supervisión es el de asegurar que el Control Interno funciona adecuadamente, a través de dos modalidades: a) Actividades continuas, y, b) Evaluaciones puntuales.

Las primeras son aquellas que están incorporadas a las actividades normales y recurrentes que, ejecutándose en tiempo real y arraigadas a la gestión, generan respuestas dinámicas a las circunstancias que sobrevienen.

En cuanto a las evaluaciones puntuales, incluyen algunas consideraciones:

a) Su alcance y frecuencia está determinado por la naturaleza e importancia de los cambios y riesgos que conllevan, la competencia y experiencia de quienes aplican los controles, y los resultados de la supervisión continuada.

b) Son ejecutadas por los propios responsables de las áreas de gestión (auto-evaluación), la auditoria interna (incluida en el planeamiento o solicitada especialmente por la dirección), y los auditores externos.

La tarea del evaluador es la de averiguar el funcionamiento real del sistema; es decir, que existan los controles y estén formalizados, que se apliquen cotidianamente como una rutina incorporada a los hábitos, y que resulten aptos para los fines perseguidos. (12)

El COSO ERM es aplicable a todo tipo de entidades tanto lucrativas como no lucrativas y su enfoque en evaluar y mejor sus sistemas de control interno y evitar riesgos futuros.

3.7 METODOLOGÍA COBIT

COBIT (Control de Objetivos para la Tecnología de Información) fue iniciativa llevada a cabo por el Instituto de Gobierno de Tecnología de Información. Este instituto fue creado en el año 1998 en los Estados Unidos de América, y su objetivo fundamental es establecer normas y lineamientos paa la utilización de la tecnología de información.

COBIT ha sido desarrollado como una norma generalmente aplicable y marco aceptado para las buenas prácticas de seguridad y control de la tecnología de información que proveen una referencia para la administración, los usuarios, y los que ejercen la Auditoria de Sistemas de Información, el control y la seguridad de TI. (8:1)

COBIT es una herramienta innovadora que toma en consideración las mejores prácticas para la evaluación del manejo, administración y evaluación de la tecnología de información, vinculando los distintos procesos del negocio con los recursos informáticos que los sustentan. También trata sobre los procesos de aseguramiento de la auditoria de TI, los cuales pueden resumirse como:

- Obtener una comprensión de los requerimientos del negocio, riesgos relacionados y medidas de control relevantes.
- Evaluar lo adecuado de los controles establecidos
- Evaluar el cumplimiento a través de pruebas, sobre los controles establecidos.

COBIT comprende la evaluación de Tecnología de Información desde 4 áreas y treinta y cuatro procesos. Los dominios son: Planeación y Organización (11 objetivos), Adquisición e Implementación (6 objetivos), Entrega Servicios y Soporte (13 objetivos) y Monitoreo (4 objetivos).

Al considerar los 34 objetivos de control de alto nivel, las organizaciones pueden asegurar que cuentan con una estructura adecuada de gobierno y control para su entorno de TI, según el Instituto de Gobierno de Tecnología de Información. (8:22)

COBIT, está dirigido a la dirección y al personal que provee servicios de información, departamentos de control y que realice funciones de auditoría.

3.8 EVALUACIÓN DEL CONTROL INTERNO

Evaluar un sistema de Control Interno, significa hacer una evaluación objetiva del mismo. Esta evaluación se realiza a través de la interpretación de los resultados de ciertas pruebas relacionadas, que son realizadas para verificar y comprobar si las políticas, métodos, sistemas y procedimientos aprobados para salvaguardar los activos y para hacer eficiente las operaciones, han sido aplicados apropiadamente.

3.9 MÉTODOS DE EVALUACIÓN DEL CONTROL INTERNO

La evaluación del Control Interno puede efectuarse aplicando los siguientes métodos: (11)

1. Descriptivo o Narrativo
2. De Cuestionario
3. Gráfico

3.9.1 Método Descriptivo o Narrativo

El método descriptivo, como su nombre lo indica, consiste en describir las diferentes actividades de los departamentos, de los funcionarios y empleados, y los registros aplicados mediante el sistema manual o computarizado. Sin embargo, no debe incurrirse en el error de describir esas actividades en forma aislada; por el contrario, se hace necesario incorporar y aplicar procesos de recorrido a las operaciones describiendo los pasos, actividades y procesos, deberes y responsabilidades siguiendo el flujo y traslado de datos, informes y documentos a través de su manejo en los departamentos citados.

Por consiguiente, implica la descripción detallada de los procedimientos más importantes y las características del sistema de Control Interno para las distintas áreas, enfatizando sobre los registros y formularios que intervienen en el sistema.

En otras palabras, refiere la descripción de las actividades y procedimientos utilizados por el personal en las diversas unidades operativas, administrativas y financieras que conforman la empresa, haciendo referencia a los sistemas o registros relacionados con esas actividades y procedimientos; la descripción debe hacerse de manera tal que confirme las situaciones imperantes, las ventajas y fortalezas de los sistemas y procedimientos y en las funciones del personal, como las fallas y debilidades en los mismos; nunca se practicará este método en forma aislada o con subjetividad.

Es importante detallar ampliamente y por escrito, los métodos contables y administrativos en vigencia, mencionando los registros y formas contables utilizadas, los empleados que los manejan, las personas que custodian los bienes, y cuanto perciben por sueldos y otras remuneraciones. La información se obtiene y se prepara según lo juzgue conveniente el Auditor Interno, ya sea por procedimientos, departamento y funciones, o por algún proceso que sea adecuado a las circunstancias de la evaluación.

El éxito en la aplicación de este método se basa en la tenencia o levantamiento de un inventario que incluya todos los procedimientos operativos, administrativos y financieros de la empresa, lo cual permitirá una mejor planificación del orden y prioridad de la evaluación. También, la forma y extensión en la aplicación de este método dependerá de la práctica y juicio del Auditor Interno, y que puede consistir en:

- Preparar las notas relativas al estudio de la empresa de tal manera que cubra todos los aspectos de su revisión.
- Que las notas relativas contengan observaciones únicamente respecto de las deficiencias del Control Interno y las Recomendaciones, ambas formando parte de sus papeles de trabajo, y también cuando el control existente en otras secciones no cubiertas por sus notas, no sea el adecuado.

- Cuidado en el orden de evaluación, teniendo en cuenta la operación en la unidad o área de trabajo precedente y su impacto en la unidad siguiente.

VENTAJAS

- El estudio es bastante detallado de cada operación; esto permite obtener un mejor y mayor conocimiento de la empresa.
- Obliga al Auditor Interno a realizar un esfuerzo mental hacia el análisis y investigación de las situaciones establecidas.

DESVENTAJAS

- Algunas situaciones importantes inadvertidas
- No se cuenta con un índice de eficiencia.

3.9.2 Método de Cuestionario

Consiste en utilizar como instrumento para la investigación, cuestionarios previamente elaborados y diseñados que involucran preguntas acerca de la forma como se ejecutan las transacciones u operaciones así como de las personas que intervienen en su manejo; asimismo, la forma en que fluyen las operaciones a través de los diferentes puestos o lugares en donde se definen y/o se determinan los procedimientos de control para la conducción de las operaciones.

Este método define la evaluación a base de preguntas, cuyas respuestas son emitidas directamente por los responsables de las distintas áreas de trabajo bajo examen. Por medio de las respuestas, se obtiene evidencia a constatar con procedimientos alternos que ayudarán a determinar si los controles operan tal como fueron diseñados y establecidos.

La aplicación de estos cuestionarios ayuda significativamente a determinar las áreas críticas de una manera uniforme y confiable.

Las preguntas del cuestionario requieren información respecto a cómo se efectúa el manejo de las operaciones, quién tiene a su cargo las funciones, los tiempos, movimientos, los pasos y actividades. Los cuestionarios son elaborados de tal manera que las respuestas afirmativas indican la existencia de una adecuada medida de control, mientras que las respuestas negativas señalan una falla o debilidad en el sistema establecido.

3.9.3 Método Gráfico

También llamado de flujo-gramas, consiste en revelar o describir la estructura orgánica de las áreas en examen y de los procedimientos utilizando símbolos convencionales y explicaciones con ideas completas de los procedimientos de la empresa.

Señala por medio de cuadros y gráficas el flujo de las operaciones a través de los puestos o lugares en donde se encuentran establecidas las medidas de control para el ejercicio de las operaciones.

Este método permite detectar con mayor facilidad los puntos en donde se encuentran y concentran las debilidades de control, aún cuando habrá de reconocerse que se requiere de mayor inversión de tiempo por el Auditor Interno en la elaboración de los flujo-gramas y en la habilidad o especialización para su preparación.

Por ello, se recomienda el uso de la carta o gráfica de organización que según el autor George R. Terry, son cuadros sintéticos que indican los aspectos más importantes de una estructura de organización, incluyendo las principales funciones y sus relaciones, los canales de supervisión y la autoridad relativa de cada empleado encargado de su función respectiva.

Existen dos tipos de gráficas de organización:

1. Cartas Maestras: Que presentan las relaciones existentes entre los principales departamentos.

2. Cartas suplementarias: Que muestran (cada una), la estructura por departamento en forma más detallada.

Se recomienda el uso combinado de estas cartas con los manuales de operación puesto que ambos se complementan.

VENTAJAS

- Proporciona una rápida visualización de la estructura del negocio.
- Identifica la ausencia de controles financieros y operativos.
- Permite una visión panorámica de las operaciones o de la entidad.
- Identifica desviaciones de procedimientos (hallazgos importantes y menores según la importancia relativa).
- Identifica procedimientos inútiles que sobran o que faltan.
- Facilita el entendimiento de las recomendaciones del Auditor Interno a la Gerencia sobre asuntos contables o financieros.
- Asegura la integridad y exactitud de las operaciones realizadas por el ente económico.

DESVENTAJAS

- Pérdida de tiempo cuando no se está familiarizado a este método o no cubre las necesidades del Auditor Interno.
- Dificultad para realizar cambios o modificaciones, ya que es necesario su nueva preparación.

3.10 DEFINICIÓN DE CONTROL INTERNO INFORMÁTICO

Es una herramienta enfocada a la adecuada gestión de los sistemas de información; controla que todas las actividades de sistemas sean realizadas cumpliendo con los procedimientos y normativas establecidas y aprobadas por la administración de la empresa. (7:131)

Este tipo de control constituye el sistema integrado al proceso administrativo, en la planeación, organización, dirección y control de las operaciones con el fin de asegurar la protección de los recursos informáticos y mejorar los índices de economía, eficiencia y efectividad de los procesos operativos automatizados.

3.11 IMPORTANCIA

Ayuda a medir la eficiencia y la productividad al momento de implantar controles internos en la empresa.

3.12 OBJETIVOS

- **Establecer como prioridad la seguridad y protección de la información, del sistema computacional y de los recursos informáticos de la empresa. (7:135)**

Este objetivo pretende establecer las pautas que sirven para proteger y manejar adecuadamente la información y los recursos informáticos. Con la implementación del control interno informático se pretende vigilar que se cumpla con la protección y seguridad de los bienes y activos de la empresa, estableciendo todas las medidas, planes, programas, métodos, técnicas y funciones que permitan, administrar adecuadamente sus activos. Otra de las funciones importantes del control interno informático es vigilar y evaluar las adhesiones, utilización, protección, custodia y

resguardo correcto de aquellos bienes informáticos que permitirán valorar su óptimo aprovechamiento en la empresa.

- **Promover la confidencialidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes de la empresa. (7:135)**

Significa que debe verificarse que los activos informáticos estén correctamente registrados, debidamente cuantificados y saber donde están ubicados; esto se logra a través de una inscripción contable adecuada de las transacciones comerciales de la empresa y del registro oportuno de sus movimientos.

- **Implementar los métodos, técnicas y procedimientos necesarios para coadyuvar al eficiente desarrollo de las funciones, actividades y tareas de los servicios computacionales, para satisfacer los requerimientos de sistemas en la empresa.(7:135)**

Este objetivo contribuye a la implantación y aplicación correcta de los métodos, técnicas y procedimientos que ayuden a evaluar y, en su caso, retroalimentar la realización adecuada de las funciones, actividades y tareas encomendadas a las áreas de sistematización de una empresa.

- **Instaurar y hacer cumplir las normas, políticas y procedimientos que regulen las actividades de sistematización de la empresa.(7:135)**

Para que se lleven a cabo las actividades de sistematización en una empresa, se debe vigilar que se cumplan de manera adecuada las disposiciones, reglamentos y normas que regulan el desarrollo de tales actividades, además de tener que cumplir con los métodos, técnicas y procedimientos previamente determinados.

- **Establecer las acciones necesarias para el adecuado diseño e implementación de sistemas computarizados, a fin de que permitan proporcionar eficientemente los servicios de procesamiento de información en la empresa. (7:135)**

Contribuye a la implementación y diseño de los sistemas de la empresa; esto únicamente se logra cuando se conocen las funciones y actividades que desarrolla la empresa.

Con la presentación de los objetivos anteriores solo se busca ejemplificar los aspectos básicos que se deben considerar al implantar el control interno informático de una empresa. El propósito es que se tome en cuenta dicho control para su aplicación real en la institución, en el entendimiento de que los objetivos se pueden diseñar y adaptar de acuerdo a las necesidades que surjan.

No se debe perder de vista que el control interno informático busca verificar, evaluar y, en su caso, retroalimentar la protección de los activos informáticos de la empresa, el registro adecuado de sus operaciones contables y la emisión de sus resultados, así como evaluar sus funciones, actividades y tareas.

3.13 FUNCIONES

El Control Interno Informático controla diariamente que todas las actividades de los sistemas de información sean realizadas cumpliendo con los procedimientos, y normativas aplicables aprobadas por la Administración de la empresa y/o la dirección informática, así como los requerimientos legales.

La función del Control Interno Informático es asegurar que las medidas de los mecanismos implantados por cada responsable sean válidas y correctas.

El Control Interno Informático suele ser desempeñado por un órgano a nivel de staff de la Dirección del Departamento de Informática y está dotado del personal especializado y de los medios materiales relacionados a los objetivos previstos.

Constituyen principales objetivos del Control Interno Informático:

- Controlar que todas las actividades se realicen cumpliendo con los procedimientos y normas aprobados y debidamente establecidos, evaluar su bondad y asegurar el cumplimiento de las normas legales.
- Asesorar sobre el conocimiento de las normas.
- Colaborar y apoyar el trabajo de Auditoria Informática, así como de las Auditorías Independientes al grupo.
- Definir, implantar, ejecutar mecanismos y controles para comprobar el buen servicio informático.

En consecuencia, la Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias que permiten determinar si un sistema automatizado salvaguarda los activos, mantiene la integridad de los datos, contribuye eficazmente al logro de los fines de la organización y utiliza eficientemente los recursos.

La evaluación del Control Interno Informático forma parte de las funciones de Auditoría Interna, quien desempeña un papel importante en la correspondiente evaluación. Por otra parte, la evaluación hecha por los auditores externos también constituye un elemento importante para determinar su eficacia.

El Auditor Interno es un profesional que trabaja en el ámbito interno de la empresa y entre los objetivos que persigue se encuentra la evaluación del Control Interno Informático, como base esencial de verificación y comprobación del buen desempeño de las operaciones. Su trabajo de auditoría comprende el examen y evaluación de la efectividad del sistema de Control Interno Informático y de su eficacia para alcanzar los objetivos establecidos por la Administración.

Los Auditores Internos deben revisar la confiabilidad e integridad de la información financiera, administrativa y operativa, y los medios utilizados para identificar, medir, dosificar y divulgar dicha información. Algunas de las funciones más importantes de los Auditores Internos para la evaluación del Control Interno Informático, se incluye:

- Planear, dirigir y organizar los procesos de revisión, verificación y evolución del sistema de control.
- Verificar que el sistema de control esté formalmente establecido y aprobado dentro de la organización, y que su aplicación sea intrínseco al desarrollo de las funciones de cada empleado y, en particular de aquellos que tengan responsabilidad de los sistemas informáticos.
- Velar por el cumplimiento de las leyes, normas, políticas, procedimientos, planes, programas, proyectos y metas que requieran los sistemas informáticos y recomendar los ajustes, cambios y mejoras que sean necesarios.
- Mantener permanentemente informados a los Directivos acerca del estado de funcionamiento, efectividad del control, exponiendo con claridad y detalle las debilidades detectadas, las fallas de cumplimiento, pero principalmente, las recomendaciones, los cambios, mejoras a incorporar con el fin de eliminar los riesgos, causas y origen.
- Verificar que se implanten las acciones correctivas y las recomendaciones sugeridas.

3.14 ELEMENTOS

- **Controles Internos sobre la organización del Área Informática. (7:137)**

Este elemento, busca determinar que la estructura de organización del área de sistemas automatizados sea la más apropiada para funcionar con eficiencia y

eficacia. Se logra a través de la incorporación y aplicación de un diseño adecuado a la estructura de puestos, unidades de trabajo, líneas de autoridad y canales de comunicación, complementados con la definición correcta de funciones y actividades, la asignación de responsabilidades y la definición clara de los perfiles de cada puesto. Este elemento, incluye:

- ✓ Dirección.
- ✓ División del Trabajo.
- ✓ Asignación de responsabilidades y de autoridad.
- ✓ Establecimiento de estándares y métodos.
- ✓ Perfiles de puestos.

- **Controles Internos sobre el Análisis, desarrollo e implantación de sistemas. (7:145)**

Las actividades que realizan las empresas para el análisis, diseño, desarrollo e implantación de sistemas son únicas y por lo tanto, no tienen parecido alguno con otras actividades. Este elemento de Control Interno Informático, incluye:

- ✓ Estandarización de metodologías para el desarrollo de proyectos.
- ✓ Asegurar que el beneficio de los sistemas sea el óptimo.
- ✓ Elaborar estudios de factibilidad del sistema.
- ✓ Garantizar la eficiencia y eficacia del análisis y diseño de sistemas.
- ✓ Vigilar la efectividad y eficiencia en la implantación y mantenimiento del sistema.
- ✓ Optimizar el uso del sistema por medio de su documentación.

- **Controles Internos para la operación del sistema. (7:157)**

Este elemento evalúa, verifica el funcionamiento y eficacia de los sistemas automatizados, bajo condiciones con características muy especiales. Adopta un elemento de vigilancia, verificación, ayuda a garantizar el cumplimiento de los objetivos básicos del Control Interno, a prevenir, eliminar, evitar errores y deficiencias de operación, así como el posible uso fraudulento de la información que se procesa en un centro de cómputo, además de posibles robos, piratería, alteración, modificaciones de la información de los sistemas y programas de la empresa. Su aplicación y funcionamiento se extiende al uso, conservación, mantenimiento, seguridad de los equipos (Hardware) y sistemas de procesamiento asignados al área de sistemas; es decir, no solo al aspecto físico del equipo (hardware) y de las instalaciones, sino que también del aspecto lógico, la información y a los recursos humanos, e incluye:

- ✓ Prevenir y corregir los errores de operación.
- ✓ Prevenir y evitar la manipulación fraudulenta de la información.
- ✓ Implementar y mantener la seguridad en la operación.
- ✓ Mantener la confiabilidad, oportunidad, veracidad y suficiencia en el procesamiento de la información de la empresa.

- **Controles internos para los procesos de entrada de datos, de información y emisión de resultados. (7:160)**

Un sistema de información involucra un procedimiento de entrada, de proceso y de salida de datos. Un dato de entrada se transforma en información útil de salida mediante algún proceso interior del sistema. El Control Interno Informático es útil para verificar que este procedimiento se aplique correctamente y con todas las medidas de seguridad posibles que permitan garantizar la confiabilidad en el sistema, e incluye:

- ✓ Verificar la existencia y funcionamiento de los procedimientos de captura de datos.
- ✓ Comprobar que todos los datos son debidamente procesados.
- ✓ Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos.
- ✓ Comprobar la oportunidad, confiabilidad y veracidad en la emisión de los resultados del procesamiento de información.

- **Controles internos Sobre la Seguridad del Área de Sistemas. (7:164)**

En el contexto hay ciertos aspectos fundamentales a considerar en el diseño de cualquier centro de informática, tales como la seguridad de sus recursos informáticos, del personal y de la información de sus programas. Conforme a medidas preventivas o correctivas, o mediante el diseño de programas de prevención de contingencias para la eliminación o disminución de riesgos, se logra la seguridad de los sistemas. Este elemento incluye:

- ✓ Controles para prevenir, evitar amenazas, riesgos y contingencias que inciden en el área de sistematización.
- ✓ Controles para la seguridad física del área de sistemas.
- ✓ Controles para la seguridad lógica de los sistemas.
- ✓ Controles para la seguridad de las bases de datos.
- ✓ Controles para la seguridad en la operación de los sistemas automatizados.
- ✓ Controles para la seguridad del personal.

La información del área de sistemas es unos de los activos más valiosos de la empresa; en consecuencia, todas las medidas que se adopten para la prevención de contingencias son de vital importancia en beneficio de la protección de los activos.

- **Controles para prevenir y evitar las amenazas, riesgos y contingencias en las áreas de sistematización. (7:167)**

Con el fin de prevenir repercusiones de posibles amenazas, riesgos y contingencias es necesario identificar aquellas situaciones que puedan influir en la seguridad de las instalaciones, sus programas e información relacionada, así como del personal que los opera, ayudando a identificar eventualidades que puedan presentarse en dichas áreas. Es también muy importante prevenir posibles contingencias antes que ocurran, así como ejercer el control suficiente en los casos de ocurrencia, o corregirlos inmediatamente después que suceden. Existen a disposición en el mercado, gran cantidad de medios para el control y prevención de contingencias en los sistemas informáticos, los cuales son seleccionados y adquiridos por las empresas de acuerdo a sus características, necesidades y condiciones específicas de procesamiento de información, pero más aún porque se adecúen o estén hechos a la medida de sus operaciones. Algunos controles básicos adoptados en las áreas de sistematización para evitar amenazas a los sistemas, a su información, programas y recursos informáticos, se describen a continuación:

- ✓ Control de acceso físico del personal al área de cómputo.
- ✓ Control de acceso al sistema, a las bases de datos, a los programas (software) y a la información.
- ✓ Uso de niveles de privilegios para acceso.
- ✓ Monitoreo de accesos de usuarios, información y programas en uso.
- ✓ Existencia de manuales e instructivos, así como difusión y vigilancia del cumplimiento de los reglamentos del sistema.
- ✓ Identificación de los riesgos y amenazas para el sistema para adoptar las medidas preventivas necesarias.
- ✓ Elaboración de planes de contingencia, simulacros y bitácoras de seguimiento.

- **Controles para la seguridad física del área de sistemas. (7:168)**

Este tipo de controles busca salvaguardar los activos tangibles de la empresa tales como la sistematización para la protección y custodia de los equipos de cómputo (hardware), periféricos, mobiliario y equipo a esa área, así como la protección y seguridad del personal, de los usuarios y en general del personal del centro de cómputo. Algunos controles básicos adoptados en las áreas de sistematización para la protección de sus recursos, aún cuando las empresas determinan los mismos de acuerdo con sus características, necesidades y condiciones específicas de procesamiento de información, se describen a continuación:

- ✓ Inventario del equipo (hardware), mobiliario y equipo.
- ✓ Resguardo del equipo de cómputo.
- ✓ Bitácoras de mantenimientos y correcciones.
- ✓ Acceso registrado del personal al área de sistemas.
- ✓ Mantenimiento a instalaciones y construcciones.
- ✓ Seguros y fianzas para los equipos y programas.
- ✓ Contratos de actualización, asesoría y mantenimiento de equipos (hardware).

- **Controles para la seguridad lógica de los sistemas. (7:172)**

También es necesario establecer controles y medidas preventivas y correctivas para salvaguardar los bienes lógicos de la empresa; en otros términos, los bienes intangibles de los centros informáticos. Se pretende tener un buen uso de los programas (software), los sistemas operativos, del procesamiento de la información, de los accesos al sistema, y de los privilegios y restricciones de los usuarios.

Estos controles se establecen de acuerdo al tipo de sistema de la empresa, al tamaño y configuración del equipo (hardware), a la forma de procesamiento de la información y de las características concretas y procedimientos de operación, e incluyen:

- ✓ Inventario de programas (software).
- ✓ Acceso al sistema, a los programas y a la información.
- ✓ Establecimiento de niveles de acceso.
- ✓ Dígitos verificadores y cifras de control.
- ✓ Palabras claves de accesos
- ✓ Controles para el seguimiento de las secuencias rutinarias lógicas del sistema.

- **Controles para la seguridad de las bases de datos. (7:173)**

Estos controles se basan en la protección de la información a cargo del área de sistemas de la empresa, ya sea través de las medidas de seguridad y del control, que limiten el acceso y uso de esa información, o mediante sus respaldos periódicos *(back ups)* con el fin de mantener su confidencialidad y de prevenir alteraciones, descuidos, robos y otros actos delictivos que afecten su manejo. Las bases de datos constituyen los activos más importantes de las empresas porque contienen la información que se captura y procesa, y por lo tanto, se deben proteger adecuadamente. Con las restricciones de acceso al sistema se evitan posibles alteraciones, uso fraudulento, piratería, destrucción y sabotaje de la información. Estos controles pueden ser establecidos por el área administrativa vigilando el acceso de los usuarios al sistema, protegiendo la información a través de respaldos periódicos *(back ups)* y programas para la recuperación de datos en caso de pérdida, deterioro y de cualquier mal uso que se haga de ellos. Los siguientes son algunos de los controles que se pueden establecer para la seguridad de las bases de datos de la empresa:

- ✓ Programas de protección para impedir el uso inadecuado y la alteración de datos de uso exclusivo.
- ✓ Respaldos periódicos de información *(back ups)*.
- ✓ Planes y programas para prevenir contingencias y recuperación de la información.
- ✓ Control de accesos a las bases de datos.
- ✓ Rutinas de monitoreo y evaluación de operaciones relacionadas con las bases de datos.

- **Controles para la seguridad en la operación de los sistemas automatizados. (7:175)**

Estos tipos de controles se refieren al acceso y aprovechamiento por el personal informático y de los usuarios, de la información contenida en las bases de datos. Para obtener un buen funcionamiento de los sistemas de procesamiento de datos, es necesario establecer controles y medidas preventivas contra accidentes, actos dolosos premeditados o negligencias que repercuten en la operación y funcionamiento del sistema; algunos controles para la seguridad en la operación del sistema, se describen a continuación:

- ✓ Para los procedimientos de operación.
- ✓ Para el procesamiento de información.
- ✓ Para la emisión de resultados.
- ✓ Específicos para la operación de la computadora.
- ✓ Para la emisión de resultados.
- ✓ Para el almacenamiento de la información.
- ✓ Para el mantenimiento del sistema.

- **Controles para la seguridad del personal. (7:176)**

Se refieren a la seguridad y protección de los operadores, analistas, programadores y demás personal que está en contacto directo con el sistema, así como a la seguridad de los usuarios y beneficiarios de la información, desde la dirección hasta la operación de sus áreas y equipos. Es indispensable el establecimiento de Controles Internos Informáticos en las empresas a fin de ayudar a proteger y salvaguardar la seguridad de los activos; entre los principales controles se encuentran:

- ✓ Controles administrativos del personal.
- ✓ Planes y programas de capacitación.

3.15 RIESGOS

Se define como la posibilidad de ocurrencia de errores significativos o irregularidades de los sistemas de información y de que no sean descubiertos oportunamente por medio de procedimientos de control de las empresas. Los errores incluyen todas las clases de equivocaciones (no intencionales) tales como, la posibilidad de equivocación en la interpretación de principios contables y del reconocimiento de hechos. Las irregularidades son falsas exposiciones (intencionales) de la gerencia o de los empleados, que en muchas ocasiones implican la sustracción y pérdida de los activos propiedad de las empresas. El riesgo de Control Interno Informático está integrado por:

- **Riesgo Inherente:** La posibilidad de que en el proceso contable (registro de las operaciones y preparación de estados financieros) ocurran errores sustanciales antes de considerar la efectividad de los sistemas de control.
- **Riesgo de Control:** La incapacidad de los Controles Internos Informáticos en cuanto a prevenir o detectar los errores o irregularidades sustanciales de los sistemas de información.

- **Riesgo de Detección:** La posibilidad que hayan ocurrido errores importantes en el proceso administrativo-contable y que no sean detectados por el Control Interno Informático y tampoco por las pruebas y procedimientos diseñados por el Auditor Interno.

3.16 MEDICIÓN DEL RIESGO

Al concebir los posibles riesgos de un área en específico de una empresa, debe efectuarse la evaluación de los mismos. Se han establecido dos aspectos para realizar la medición de los riesgos identificados:

- **Probabilidad,** es la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia o teniendo en cuenta la presencia de factores internos y externos que puedan propiciar el riesgo.

- **Impacto,** la consecuencia que puede ocasionar a la organización la materialización del riesgo.

3.17 MATRIZ DE RIESGOS

Es un documento en el cual se asigna calificación de acuerdo a criterios a las diferentes operaciones realizadas en la empresa. Los criterios utilizados generalmente son a mayor cantidad de errores, se obtendrá una calificación de riesgo superior. Una matriz de riesgo constituye una herramienta de control y de gestión normalmente utilizada para identificar las actividades (procesos y productos) más importantes de una empresa. La matriz de riesgos tiene una probabilidad de ocurrencia a nivel de impacto de riego alto, medio y bajo.

3.18 CLASIFICACIÓN

Los Controles Internos Informáticos se clasifican en:

- **Controles Preventivos:** Los que eliminar o reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de infracciones, para tratar de evitar el hecho. Un ejemplo claro, podría ser un programa (*software*) de seguridad que impida los accesos no autorizados al sistema.

- **Controles Detectivos:** Los que no evitan que ocurran las causas del riesgo, sino que los detecta luego de ocurridos. En cierta forma sirven para evaluar la eficiencia de los controles preventivos; por ejemplo, el registro no autorizado de intentos de acceso a los programas informáticos.

- **Controles correctivos:** Aquellos que ayudan a la investigación, eliminación y corrección de las causas del riesgo y permiten recuperar información cuando se han producido incidencias; por ejemplo, la recuperación de un programa dañado por medio de las copias de seguridad.

CAPÍTULO IV

EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO DEL ÁREA DE SEGURIDAD DEL DEPARTAMENTO DE SISTEMAS DE UNA INDUSTRIA DE CALZADO

4.1 CASO PRÁCTICO

El caso práctico a continuación, está referido a la evaluación del Control Interno Informático del área de Seguridad del Departamento de Sistemas de la empresa Calzado Cobanero, S.A., y enfatiza sobre los resultados obtenidos considerados como principales riesgos para su operación y especialmente describe las recomendaciones tendientes a eliminar o reducir los mismos, evitar que las deficiencias importantes establecidas le puedan afectar adversamente en su desarrollo por la desprotección, falta de confiabilidad y pérdida de la información relacionada.

Los objetivos del Control Interno Informático están dirigidos a proporcionar una seguridad razonable de que el Departamento de Sistemas cuenta con un ambiente de registro y control para el apropiado resguardo de los equipos *(hardware)*, los programas *(software)*, y el personal que los opera y administra.

Para la evaluación en referencia, fue aplicado el Método analítico y de cuestionario mediante el cual se procedió a recopilar la información, aplicando técnicas y estrategias de: a) Presentación de Cuestionarios, b) Entrevistas con el personal clave de las áreas participantes, c) Observación de las aplicaciones y procesos, d) Procesos de recorrido a los principales procedimientos del Departamento de Sistemas y en consecuencia, el examen de documentación, inspección de los bienes, comparación de datos de equipos y programas, accesos de personal, y lista de chequeo (*check list*).

Para el efecto, se realizó el Proceso de Planificación de la auditoría y como parte del mismo se incluyó la Evaluación del Control Interno Informático, concluyendo con el diseño de la Guía o Programa a ejecutar, estableciendo los tiempos (horas hombre) del personal participante. Mediante esta Guía, se planificó los aspectos más importantes a evaluar y los temas específicos en el área de seguridad relacionados.

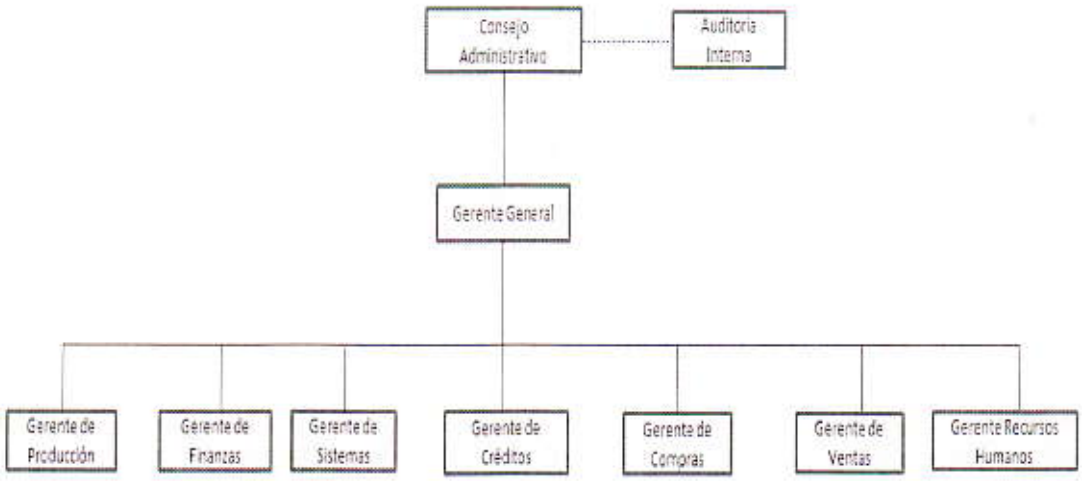
La empresa de calzado inició sus operaciones en el año 1914, como una tiñeria y posteriormente se convirtió en una zapatería. En el año 1965 cambió su nombre por el de Calzado Cobanero, S.A., con fines de fabricar zapato de trabajo de uso diario, botas para trabajadores industriales, suelas y adhesivos. El proceso de producción se inicia desde que las pieles ingresan a la tiñería, secado y lijado, luego de la zapatería al departamento de corte, preparación, despunte, montado, lijado y empaque; finalmente, el producto terminado es trasladado a la bodega para su distribución a diversos lugares de comercialización y venta.

Actualmente produce de 3,000 a 3,400 pares de zapatos al día, generando empleo para más de 1,000 personas. Las oficinas centrales se ubican en la zona 12 de la ciudad de Guatemala y cuenta con tres plantas de producción, dos en Guatemala y una en Costa Rica.

4.2 ESTRUCTURA ORGANIZACIONAL

La estructura organizativa es de la siguiente forma: Consejo administrativo, Gerente General, Auditoría Interna, Gerente de Producción, Gerente Financiero, Gerente Compras, Gerente Ventas, Gerente Administrativo, Gerente de Sistemas y Gerente Créditos.

ORGANIGRAMA 1
CALZADO COBANERO, S.A.



Fuente: Propia

El departamento de Sistemas se conforma de la siguiente manera: Gerente de Sistemas, Sub-Jefe Sistemas, Programador y Soporte Técnico.

ORGANIGRAMA 2
GERENCIA DE SISTEMAS

Fuente: Empresa Calzado Cobanero, S.A

4.2.1 Planeación de la Auditoria Interna.

1. Objetivo General

Verificar la efectividad y la eficacia de los controles internos en aplicación al cumplimiento de las políticas aprobadas y establecidas para salvaguardar los equipos, programas y personal, asi como la confiabilidad de los procesos y sistemas de información.

2. Objetivos Especificos

Establecer la propiedad de la seguridad y protección de la información, del sistema computacional de los recursos informáticos de la empresa, el cumplimiento de los planes, programas, estándares, políticas, normas y lineamientos que regulan las funciones y actividades de seguridad en las áreas de sistemas de procesamiento de información, así como del personal y de los usuarios del centro de información.
Determinar si los sistemas y procedimientos proporcionan la integridad, confiablidad de la información, seguridad del personal, equipos (hardware) y programas (software) e instalaciones, y la apropiada custodia de los activos para asegurar la inexistencia de usos no autorizados y de la disposición ilegal de los mismos.

3. Puntos a Evaluar en el Control Interno Informático

De acuerdo a los objetivos planteados para realizar la auditoria y considerando algunos factores o debilidades observadas mediante las otras auditorias que se han efectuado cada año, nos enfocaremos en evaluar el control interno informático sobre la seguridad. La metodología que aplicaremos es en base al COSO ERM (Gestión de Riesgos Empresarial).

- ✓ Evaluación de Claves y Acceso del personal interno y externo.
- ✓ Evaluación de la seguridad en equipos (Hardware).
- ✓ Evaluación de la seguridad en programas (Software).
- ✓ Evaluación de la seguridad en instalaciones, mantenimientos y seguros.
- ✓ Verificar el plan de contingencia.

4. PLANES Y PROGRAMAS

De acuerdo a los puntos que serán evaluaos, y en consecuencia de los objetivos, la estratégica para realizar la evaluación del control interno informático, se han diseñado las etapas, eventos y tareas que serán necesarias para desarrollar nuestra auditoría interna.

Estrategia para la evaluación del control interno informático: durante la visita preliminar se procederá a observar y obtener información sobre la seguridad con el que cuenta el departamento de sistemas, se utilizara un cuestionario previamente elaborado, se entrevistara al personal del área. El objetivo final es verificar sus controles y detectar sus posibles debilidades.

Etapas, eventos y tareas:

- ✓ **Etapas:** De acuerdo a la metodología utilizada, la auditoria se subdividirá en la etapa que trata esta planificación, ejecución y la presentación del informe de auditoría interna.
- ✓ **Eventos:** Para llevar un buen termino de cada etapa, se han diseñado los eventos necesarios, asignado para ello un intervalo de tiempo.
- ✓ **Tarea:** El auditor asignado deberá cumplir con las responsabilidades asignadas, en el periodo corresponde.

Los anteriores conceptos se encuentran detallados en la grafica de Gantt, que se presenta a continuación.

	Área a Evaluar: Departamento de Sistemas (La Seguridad) **Objetivos de la Auditoría:** Evaluar el Control Interno Informático, verificar la efectividad y la eficacia de los controles internos en aplicación, cumplimiento de las políticas aprobadas y establecidas para salvaguardar los equipos, programas y personal, así como la confiabilidad de los procesos y sistemas de información. **Periodo a Revisar:** Del 01 de enero al 31 diciembre de 2009	**Personal Asignado**	Karin Figueroa Auditora	Marilu Ávila O. Asis. de Auditoria	
	DESCRIPCIÓN DE ACTIVIDADES **Período de Revisión**		Del 01 al 29-01-2010		
			SEMANAS		
I.	**Administración de la Auditoría**	1	2	3	4
1	Elaborar plan de auditoría.				
2	Aprobar el plan de auditoría.				
3	Familiarización de la seguridad del Departamento de Sistemas				
4	Contestación del Cuestionario de la Evaluación del Control Interno Informático				
5	Elaboración de cédulas narrativas				
6	Evaluación del Control interno informático de la seguridad del Área de sistemas				
7	Preparación del programa de auditoria				
II.	**Desarrollo de Auditoría**				
1	Revisión de Claves y Accesos del personal Interno y Externo.				
2	Revisión de la Seguridad en Equipos (Hardware)				
3	Revisión y Evaluación de la Seguridad en programas (Software).				
4	Revisión de la Seguridad en Instalaciones, Mantenimientos y Seguros.				
5	Evaluación de Riesgos y Oportunidades de Mejora.				
6	Plan de Acción				
III.	**Informe**				
1	Elaboración del Informe de auditoría				
2	Discusión de las Conclusiones y Recomendaciones				
3	Presentación del Informe de auditoría				

Preparado por:

Karin Figueroa De La Cruz

Auditor Interno

4.2.2 Guía del Caso Práctico.

CALZADO COBANERO, S.A

EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO EN EL ÁREA DE SEGURIDAD – DEPARTAMENTO DE SISTEMAS

4.2.3 Papeles de trabajo:

P.T. No.			A
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

CALZADO COBANERO, S.A.
DEPARTAMENTO DE AUDITORÍA INTERNA.

CARTA DE NOTIFICACIÓN DE LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO SOBRE LA SEGURIDAD EN EL DEPARTAMENTO DE SISTEMAS

01 de enero 2010

Ingeniero Julio Chang
Gerente del Departamento de Sistemas
Calzado Cobanera, S.A.

Apreciable Ingeniero Chang:

Conforme al Plan Anual de Trabajo de este Departamento de Auditoría Interna, sírvase tomar nota que a partir del 01 de enero 2010 procederemos a realizar la Evaluación del Control Interno Informático del Departamento a su cargo. Bajo la supervisión de mi persona, la Señorita Marilú Ávila Orellana ha sido asignada para el desarrollo de dicha evaluación, y por lo tanto, les estará visitando a partir de esa fecha. La evaluación comprenderá un período de 20 días hábiles, es decir, que será realizada del 01 al 29 de enero en curso.

La evaluación tiene como propósito principal la medición de los Factores de Riesgo, así como la emisión de las recomendaciones prácticas y realistas con énfasis en las oportunidades de mejora, entre otras cosas, la eliminación de esos factores, todo en beneficio para el Departamento a su cargo y especialmente para la administración de la empresa. Se presentará el informe en versión final para la Gerencia General de la empresa, pero previamente se emitirá en borrador para

discutirlo con Usted, para obtener su valioso aporte en ideas, comentarios y puntos de vista al contenido.

Agradeceremos toda su colaboración y la del personal a su cargo, que indudablemente contribuirán al eficaz y oportuno desarrollo de las funciones de nuestro personal.

Atentamente,

Karin Figueroa
Auditor Interno

CALZADO COBANERO, S.A.
DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A1	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

01 de enero 2010

Licenciada Marilú Ávila Orellana
Especialista en Evaluación de Sistemas
Su asignación.

Licenciada Ávila:

A continuación se describen los aspectos más importantes relacionados con su asignación para Evaluar el Control Interno Informático. También, adjunto sírvase encontrar la Guía o Programa elaborado a la medida de las operaciones de la evaluación, la cual deberá ser completada en todas y cada una de sus secciones haciendo referencias a los Papeles de Trabajo elaborados.

Trabajo a Desarrollar:

Nuestro Plan Anual de Trabajo mantiene contemplada la Evaluación del Control Interno Informático del área de Seguridad del Departamento de Sistemas de la empresa, con énfasis en la determinación de los niveles de riesgo asociados y las Recomendaciones tendientes a eliminar los mismos. La descripción de las fortalezas con que cuenta actualmente dicho Departamento, también es permisible incluirla en el informe relacionado.

Asignación, Período de tiempo y comunicación

Se tiene previsto realizar dicha evaluación en el período del 01 al 29 de enero 2010, y para el efecto, se ha comunicado del asunto al Gerente del Departamento de Sistemas solicitándole toda la colaboración del caso.

Ha sido asignada para realizar la Evaluación del Control Interno Informático sobre el área de Seguridad del Departamento de Sistemas, y para el efecto, se le solicita preparar sus hojas de inversión de tiempo y papeles de trabajo para continuar con su intervención a partir del día 04 de enero 2010.

Papeles de Trabajo e Informe

Sírvase atender todos los lineamientos y diseños de nuestros papeles de trabajo y documentación completando la Guía de trabajo adjunta. El Informe resultante de la evaluación deberá ser emitido inicialmente en borrador como base para discusión con el Gerente del Departamento. Posteriormente, de hacer todas las incorporaciones, cambios o modificaciones, será enviado a Gerencia General.

Supervisión

Los avances de la evaluación serán supervisados directamente por mi persona, por lo tanto deberá presentar los papeles de trabajo cada dos días a partir de la fecha de su intervención; todas las inquietudes y dudas pueden ser consultadas inmediatamente para mantener coordinadas las actividades planificadas.

Atentamente,

Karin Figueroa
Auditor Interno

CALZADO COBANERO, S.A.

DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A2	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

PROGRAMA GENERAL A APLICAR EN LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO

I. INTRODUCCIÓN

Este programa constituye una guía y normativa de las actividades a seguir en la Evaluación del Control Interno Informático del área de Seguridad del Departamento de Sistemas de la empresa Calzado Cobanero, es el resultado del Proceso de Planificación y Plan Anual de Trabajo de la auditoría. Este programa no debe ser considerado como un todo o restrictivo en su naturaleza, ni como substituto de su juicio y cuidado profesional que se debe tener, pero si como una valiosa herramienta de ordenamiento, coordinación de pasos y procedimientos a aplicar, cumplir y a tomar en cuenta como una base mínima de evaluación. La Seguridad en el Departamento de Sistemas es un área sensitiva que puede originar interrupciones, cortes de los equipos, programas y problemas en el personal; es por ello, que como parte de la Auditoria Interna se evaluara el control interno.

En consecuencia, es sumamente importante compenetrarse en todos los asuntos que involucra este programa para la evaluación y someter a consulta todas aquellas dudas e inquietudes resultantes para que las mismas sean resueltas inmediatamente; no se debe iniciar el trabajo de evaluación, hasta que este programa esté plenamente comprendido para su aplicación.

II. OBJETIVO DE LA EVALUACIÓN

La evaluación tiene como objetivo verificar la efectividad y la eficacia de los controles internos en aplicación, cumplimiento de las políticas aprobadas y establecidas para salvaguardar los equipos, programas y personal, así como la confiabilidad de los procesos y sistemas de información.

III. ALCANCES

La Evaluación será realizada aplicando el método analítico y de cuestionario en el ámbito de aplicación será considerado por área de importancia: a) Planes de Contingencia, b) Personal Clave y Accesos, c) Seguridad para los Equipos (*hardware*), d) Seguridad para los Programas (*Software*), y, e) Seguridad en instalaciones, mantenimiento y seguros. Los resultados serán referidos al 31 de enero del 2010.

IV. PROCEDIMIENTOS

Conforme al proceso de Planificación, se definieron los alcances mínimos para la evaluación; en consecuencia, se aplicarán procedimientos de: a) Entrevista con el personal clave del Departamento de Sistemas y de cada área de importancia, b) Revisión de la documentación indicativa del cumplimiento de los controles y de las políticas aprobadas, c) Procesos de recorrido a los sistemas y procedimientos más importantes para evaluar sus tiempos, movimientos y la documentación de soporte utilizada, d) Revisión de las instalaciones para verificar la adecuada salvaguarda de los activos, e) Verificación de la actualización constante de los procesos dos veces al año, su funcionalidad y el personal participante. A continuación los principales pasos y procedimientos incorporados a los formularios de evaluación que se deben aplicar:

Puntos a enfocar	Descripción
○ **Planes de contingencia.**	▪ Verificar si el Departamento de Sistemas cuenta con un Plan de Contingencia en caso de siniestros y desastres, y si este ha sido plenamente conocido y aprobado por la Gerencia General. ▪ Verificar si el Plan de Contingencia, incluye los procesos, programas, sistemas, procedimientos, resguardos y las medidas de acción inmediatas que permitan re-establecer las operaciones. ▪ Verificar si todo lo anterior ha sido considerado y calificado como factor crítico de éxito. Documentar si han sido realizadas las pruebas de escenarios y prácticas de desarrollo para medir la eficiencia y eficacia del Plan. ▪ Concluir con la Evaluación indicando las observaciones o desviaciones, fallas y debilidades en esta área (hallazgos importantes) y las posibles Recomendaciones a implementar.
○ **Personal Clave y Accesos y Seguridad para los Equipos (*Hardware*).**	▪ **Revisión del control para el ingreso, egreso de personal y equipos.** Verificar la actualización de los formularios utilizados y asegurar que incluyan la siguiente información: a) Fecha, hora de ingreso y egreso de las personas, b) Nombre de las personas que ingresan y acompañantes, c) Motivo del ingreso, d) Evidencia de Autorización para el ingreso y egreso de equipo.
	▪ **Inventario del Equipo de Cómputo (hardware) ubicado en el Departamento de Sistemas.** Solicitar el listado de inventario y verificar la existencia física del mismo cotejando los datos de registro en libros y la integración de la cuenta contable (No. 112-001-01-05 - Equipo de Cómputo).

Puntos a enfocar	Descripción
	▪ **Claves de acceso.** Verificar en cuanto a la utilización de claves de acceso y tarjeta electrónica: a) El listado de usuarios habilitados para el ingreso, b) La fecha de habilitación, c) Los nombres de los usuarios, d) La fecha que expira la clave, e) Las fechas de último acceso, y, f) El status de la clave.
	▪ Concluir con la Evaluación indicando las observaciones o desviaciones, fallas y debilidades (hallazgos importantes) en esta área y las posibles Recomendaciones a restablecer.
○ **Seguridad para los Programas (*Software*)**	• **Inventario de Cintas de respaldo *(back-ups)*.** Proceder a: a) Solicitar el listado de inventario correspondiente y verificar la periodicidad con que se elabora, b) Realizar pruebas de verificación de funcionalidad de las cintas y de la información que contienen, c) Comprobar si se realizan pruebas para comprobar su funcionalidad. • **La confiabilidad de la información.** a)Verificar las pruebas periódicas que se realizan para verificar la confiabilidad de la información y de los resultados que se notifican por escrito y a quien, b) Analizar los modelos de reportes para determinar la propiedad de la información que se genera, c) Entrevistar a los usuarios para conocer sus puntos de vista y utilidad de la información que reciben, d) Establecer la existencia de bitácoras de problemas y soluciones, e) Realizar pruebas en el sistema para verificar la información de salida.

Puntos a enfocar	Descripción
	• **El Inventario de *Software*.** Verificar el inventario teórico de los Programas autorizados, reuniendo la información que a continuación se describe: a) Los datos de los contratos del desarrollador o distribuidor de las licencias, b) Cantidad de Licencias, c) Nombre de cada programa y utilización, sistemas de información, usuarios y frecuencia, d) Versión y lenguaje en que está elaborado, e) Número de computadoras autorizadas y utilizadas, sin utilizar y razones, f) Personal con acceso a cada programa y razones.
	• **La Seguridad de la tecnología informática.** Proceder a evaluar: a) Las restricciones que tienen para las direcciones IP, b) Las defensas contra virus, c) Períodos de actualización, y, d) Consultas a Asesores Externos.
○ **Seguridad en instalaciones, mantenimiento y seguros.**	• **Seguridad para la protección de equipos.** Verificar que la protección sea la adecuada protección y comprobar la existencia de: a) Cámaras de Vigilancia y modo o medio de almacenamiento, b) Extintores de incendios, su facilidad en el acceso y ubicación, c) Cargas apropiadas, es decir, que no estén vencidas, d) Aire acondicionado en buen estado de funcionamiento y record de servicio, e) Mantenimientos preventivos de los equipos, f) Dispositivos para evitar inundaciones, g) Alarmas detectoras de humo y de temperatura, h) Reguladores de voltaje y UPS, i) Software y hardware específicos para el control de accesos, k) Planes de funcionalidad y prueba de escenarios. **Contratos de mantenimiento.** Verificar como mínimo la actualización y cumplimiento de los contratos, detallando todas las características de cada uno, su vigencia y pagos.

Puntos a enfocar	Descripción
	Pólizas de seguro. a) Verificar la actualización de los seguros y que su cobertura sea la más apropiada para reposición de los bienes asegurados en caso de siniestros o eventos indeterminados, b) Verificar que el valor total de los bienes sea equivalente al monto de la cobertura del seguro, estableciendo diferencias si las hubiera.

V. CONCLUSIÓN E INFORME

Presentación de Resultados. Los resultados de la evaluación serán expuestos mediante: a) Una Matriz de Riesgos en la que se indique con todos los detalles y pormenores de cada situación establecida, principalmente dando a conocer las causas, efectos, oportunidades de mejora, Recomendaciones, b) El plan de acción, y, c) Emitir un informe en borrador para su entrega al Gerente del Departamento de Sistemas con el fin de obtener sus puntos de vista, comentarios y opiniones, que también constituyan una contribución importante para enriquecer y fortalecer el entorno del Control Interno, obteniendo el compromiso de la implementación de las Recomendaciones.

Envió de de informe. El informe será dirigido al Consejo Administrativo con copias al Gerente General, Gerente de Sistemas y Gerente Financiero.

Bibliografía. Como un apoyo a la Evaluación se sugiere la lectura del libro "Auditoría en Información" del autor José Antonio Echenique García, y el libro "Auditoría en Sistemas Computacionales", de Carlos Muñoz Razo.

Cronograma. Para realizar la Evaluación se asignan 5 días hábiles con el fin de recolectar todos los datos, en consecuencia, se deberá iniciar el 01 de enero de 2010 y concluir el 25 de enero con la entrega del informe en versión borrador debidamente discutido con el Gerente del Departamento de Sistemas y los comentarios de éste.

Atentamente,

Karin Figueroa De La Cruz
Auditor Interno

CALZADO COBANERO, S.A.

DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A3	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

CUESTIONARIO CONTROL INTERNO INFORMÁTICO SOBRE LA SEGURIDAD DEL ÁREA DE SISTEMAS

No	PREGUNTAS A USUARIOS DEL DEPARTAMENTO DE SISTEMAS	RESPUESTAS		
		SI	NO	N/A
1	¿Los sistemas informáticos y equipos de la empresa, están configurados e instalados de forma tal que reflejan las líneas de autoridad y puestos jerárquicos?	X		
2	¿Los sistemas y equipos en la empresa, funcionan de forma eficiente, tal que los recursos son bien aprovechados y acorde a la necesidades y objetivos trazados?	X		
3	Existen procedimientos de inducción o capacitación para los usuarios de los sistemas o equipos de forma periódica o programada?		X	
4	¿Los sistemas de información de la empresa se calificarían como altamente confiables y exactos?	X		
5	¿Existen políticas de ejecución de copias de seguridad para las estaciones de trabajo de forma periódica en donde la información útil de la empresa es almacenada correctamente?	X		
6	¿Existen contratos o políticas de mantenimiento físico y lógico de forma periódica para los equipos y programas informáticos?	X		
7	¿Las contraseñas de acceso a los sistemas y programas son asignados y almacenados de forma segura, mediante procedimientos establecidos?	X		
8	¿La adquisición de programas de cómputo se realiza de acuerdo a las necesidades de la empresa?	X		
9	¿Se practican inventarios físicos y teóricos a los programas informáticos instalados en los equipos de la empresa, de forma periódica?	X		
10	¿Se toman medidas preventivas y correctivas a los hallazgos encontrados en los inventarios de programas informáticos?	X		
11	¿La empresa cuenta con normas de seguridad para el almacenamiento y uso de las licencias de programas informáticos?	X		

No	PREGUNTAS A USUARIOS DEL DEPARTAMENTO DE SISTEMAS	RESPUESTAS		
		SI	NO	N/A
12	¿Los programas informáticos instalados en los equipos de cómputo están respaldados por su respectiva licencia de uso?	X		
13	¿Se han tomado medidas para reducir el riesgo de adquisición de programas informáticos sin su respectiva licencia?		X	
14	¿Los procedimientos de compra de programas informáticos, incluyen la aprobación por parte de las respectivas líneas de autoridad de la empresa?	X		
15	¿En la administración de la información y bases de datos de la empresa, está contemplado el error humano como posible causa de pérdida y daño de los datos?	X		
16	¿Existen normas para el control y protección de los sistemas de información contra el sabotaje, extorsión, fraudes, alteración, manipulación o eliminación de datos?	X		
17	¿Dentro del presupuesto de la empresa está contemplado un rubro que represente todo lo relacionado con la administración de los recursos informáticos con que se cuentan?	X		
18	¿La adquisición de las licencias de programas informáticos es registrada contablemente tomando en consideración las actividades que realiza la empresa y las diferentes formas de licenciarse?	X		
19	¿En caso de siniestro la empresa ha tomado medidas preventivas?	X		
20	¿El personal que tiene acceso a las áreas de sistemas de la empresa tiene gafete de identificación?	X		
21	¿El acceso al área de sistemas de la empresa es restringido?	X		
22	¿Existen bitácoras de acceso a los sistemas de la empresa?	X		
23	¿Existen niveles de acceso y seguridad para los sistemas de la empresa?	X		
24	¿Los sistemas de información de la empresa producen resultados fiables y satisfactorios a las necesidades de los usuarios?	X		
25	¿Las claves de acceso a los sistemas de información se cambian periódicamente?	X		
26	¿El acceso a los sistemas de información cuenta con privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información?	X		
27	¿Se delimitan las responsabilidades en cuanto a quien está autorizado a consultar y/o modificar en cada caso la información, tomando las necesidades de seguridad pertinentes?	X		

No	PREGUNTAS A USUARIOS DEL DEPARTAMENTO DE SISTEMAS	RESPUESTAS		
		SI	NO	N/A
28	¿Los sistemas de información cuentan con sus respectivos manuales actualizados y organizados?			
29	¿Se han establecido programas y procedimientos de detección e inmunización de virus en copias no autorizadas?	X		
30	¿La empresa cuenta con equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, ups o generadores de energía?	X		
31	¿Las instalaciones cuentan con sistemas de alarma por presencia de fuego, humo, así como extinguidores de incendio?	X		
32	¿Los usuarios participan en el diseño e implementación de los sistemas?	X		
33	¿Están actualizados con el plan de continuidad del negocio?	X		
34	¿Ustedes creen que como departamento de sistemas están entrenados para recuperar o restaurar información en caso de destrucción de los activos informáticos?	X		

CALZADO COBANERO, S.A.

DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A4	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

REFERENCIAS PARA EVALUACIÓN DEL CONTRO INTERNO INFORMÁTICO

✔	Revisado a satisfacción.
©	Inspección física realizada a satisfacción.
Φ	Copia física y de respaldo, revisadas a satisfacción.
¥	Procedimiento revisado a satisfacción.
B	Funcionamiento del equipo en presencia del encargado.
µ	Confirmado con el proveedor del servicio, a satisfacción
≠	Procedimiento cumplido, verificado a satisfacción.
®	Revisado y confirmado con el usuario y deficiencias comunes
⌂	Verificado con documento de soporte
ERR	Hallazgo de Control Interno
£	Confirmado con el usuario final, a satisfacción

CALZADO COBANERO, S.A.

DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A5	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

CONTROLES APLICABLES AL INGRESO DE PERSONAL EXTERNO AL DEPARTAMENTO DE SISTEMAS

Se llevo a cabo conforme al plan y se procedió a verificar el control utilizado para el ingreso de personal externo a las instalaciones del departamento de sistemas. Los resultados se presentan a continuación:

Fecha	Persona que ingresa	Motivo del ingreso	Persona quién autorizó el ingreso	Status de la Condición	Hora Ingreso	Hora Egreso	Referencia de Evaluación
07/09/2009	Carlos Monte	Revisar problemas de acceso de claves al sistema		R/1 -Sin Autorización			⌂
10/09/2009	Luis Poca Sangre	Revisar servidor de Reportes		R/1 -Sin autorización			⌂
23/09/2009	Jennifer Palace	Revisar Impresora Multifuncional	Jovita Guzmán		09:40	10:30	✔
27/09/2009	Hugo Morales	Revisar problemas en servidor de Contabilidad		R/1 – Sin autorización			⌂
28/09/2009	María José Guzmán	Revisar problemas en servidor de Contabilidad	Jovita Guzmán		11:05	14:30	✔
01/10/2009	Henry Martínez	Revisar servidor de reportes		R/1- Sin autorización			⌂
04/10/2009	Karin Figueroa	Auditoria – Reunión Trabajo	Jovita Guzmán		08:00	13:00	✔
06/10/2009	Iván Totto	Revisar problemas de correo		R/1- Sin autorización			⌂

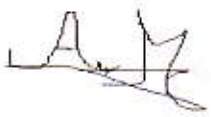
Deficiencias Establecidas

R/1 Personal que ingresó al Departamento de Sistemas sin autorización

Conclusión y Recomendación.

De ocho (8) casos evaluados, cinco (5) no cumplieron con los procedimientos aprobados y establecidos en cuanto a la autorización para el ingreso; hubo falta de requerimiento por parte del encargado. En consecuencia, el 62% de todos los casos, originan un alto riesgo de ocurrencia de accesos no autorizados; estos resultados no proporcionan una seguridad razonable de que los casos sean detectados oportunamente y corregidos de manera inmediata. Por lo tanto, los resultados de la evaluación no se consideran aceptables porque no se cumple a cabalidad con los controles, políticas y procedimientos aprobados.

Por ello, es de suma importancia instruir nuevamente al encargado sobre su responsabilidad de solicitar invariablemente a toda persona, sin distinción alguna, la autorización para el acceso al Departamento de Sistemas, presentando el formulario que evidencie la autorización respectiva, y en todo caso, comunicar inmediatamente al Gerente de Sistemas el incumplimiento en que se incurre. También, es importante documentar las soluciones implantadas para corregir estos casos de incumplimiento lo cual permitirá mantener estadísticas sobre la recurrencia.



Ana Marilú Ávila
ENCARGADO EVALUACIÓN

Vo.Bo. Karin Figueroa
AUDITOR INTERNO

CALZADO COBANERO, S.A.

DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A6	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

EVALUACIÓN DE CLAVES REQUERIDAS PARA EL ACCESO DEPARTAMENTO DE SISTEMAS

Conformé el plan de trabajo se procedió a verificar las claves de acceso utilizadas por el personal de sistemas al ingreso al departamento.

Fecha de habilitación de clave de acceso	Persona con acceso autorizado	Fecha expiración de clave	Área en el que labora	Fecha del último acceso	Status de la clave	Status de la condición	Referencia de Evaluación
01/01/2003	Ing. Julio Chang	Indefinida	Sistemas	08/10/2010	Activa	R/2 Cambio indefinido	⌂
01/01/2009	Jovita Guzmán	31/12/2010	Sistemas	08/10/2010	Activa		✔⌂
06/02/2009	Mario Rivera	31/12/2010	Sistemas	08/10/2010	Activa		✔⌂
07/06/2009	Juan Carlos Meza	31/12/2010	Sistemas	08/10/2010	Activa	R/3 La Clave corresponde a un ex empleado.	⌂

Deficiencias establecidas

R/2 La clave o *password* del Ingeniero Julio Chang no ha sido cambiada con cierta periodicidad, es decir, cada año como lo dicta el procedimiento aprobado.

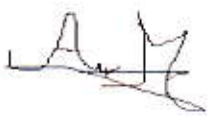
R/3 La clave corresponde a una persona que ya no labora para la empresa y que no se ha dado de baja del sistema.

Conclusión y Recomendación.

De cuatro (4) casos probados, dos (2); es decir el 50%, presentan ciertas deficiencias. Aunque la clave o *password* del ingeniero Julio Chang, Gerente del

Departamento de Sistemas tiene los mayores privilegios, no está exenta de que se ajuste al procedimiento de cambio periódico, siendo una deficiencia fácil de superar. Por lo tanto, es importante ajustarse al procedimiento establecido cambiando periódicamente la clave de acceso del Ingeniero Julio Chang, y en el caso de su ausencia, la Inga. Jovita Guzmán puede tener los accesos suficientes para superar cualquier inconveniente que surja.

Complementariamente, es también importante que la Gerencia del Departamento de Sistemas promueva los cambios inmediatos en los casos de que un colaborador termine su relación laboral con la empresa, dándole la baja en el sistema; esto eliminará el riesgo de tener accesos no autorizados.



Ana Marilú Ávila
ENCARGADO EVALUACIÓN

Vo.Bo. Karin Figueroa
AUDITOR INTERNO

CALZADO COBANERO, S.A.

DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A7	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

EVALUACIÓN DE CONTROLES PARA LA SALIDA (EGRESO) DE EQUIPO DEL DEPARTAMENTO DE SISTEMAS

Se procedió a verificar y evaluar el control interno para el egreso de equipos del departamento de sistemas.

Fecha	Identificación del Equipo	Motivo del retiro o salida	Persona quien recibe el equipo	No. de Inventario	Referencia de Evaluación
02/01/2009	Servidor de Compensación	Cambio de memoria	Paola Martinez	DS-401	®
18/06/2009	Cámara de Vigilancia	Reparación del monitor	Mario Borrayo	DS-20	®
06/10/2009	Servidor de Compensación	Cambio de memoria y disco	Mario Borrayo	DS-401	®
05/12/2009	Servidor de Logística	Cambio de fuente de poder	Paola Martinez	DS-410	®
07/12/2009	Servidor de internet y correo electrónico	Cambio de disco duro	Mario Borrayo	DS-403	®

OBS

Deficiencias establecidas

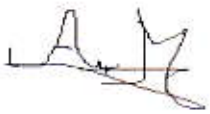
® OBS/R/4

Se evidenció la misma deficiencia en todos los casos evaluados; es decir que todos los casos no presentaron: a) Registro de las fechas en que los equipos ingresaron después de las reparaciones, b) Diagnóstico de la situación del equipo previo al retiro y/o salida y justificante para ello, c) Informe final de la reparación.

Conclusión y recomendación.

Los cinco (5) casos evaluados (el 100%) presentan deficiencias que originan el riesgo de potenciales pérdidas de los equipos; en este caso, el encargado no ha cumplido con su función de requerir los documentos suficientes y competentes tanto para la salida o retiro de los equipos como para el reingreso de los mismos, aduciendo que los registros diseñados no incluyen las casillas específicas para ello.

Es importante que se incorpore una casilla para que el encargado pueda registrar estrictamente la salida o retiro de los equipos del Departamento de sistemas; asimismo, instruirle para que requiera invariablemente de autorización escrita del Gerente de sistemas de que fueron entregados los documentos antes descritos (tanto en la salida como en el reingreso del equipo).



Ana Marilú Ávila
ENCARGADO EVALUACIÓN

Vo.Bo. Karin Figueroa
AUDITOR INTERNO

CALZADO COBANERO, S.A.

DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A8	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

REVISIÓN DEL INVENTARIO DE EQUIPOS DE CÓMPUTO EN EL DEPARTAMENTO DE SISTEMAS

Conformé al plan de trabajo se procedió a verificar el inventario de equipos ubicados en el departamento de sistemas. Este inventario fue realizado comparando los registros en libros según la integración de saldos de la cuenta 112-001-01-05 Equipo de computación. Los resultados se presentan a continuación.

Fecha Ingreso	Identificación del Equipo	Encargado del Equipo	Código del Equipo, libros contables e integración inventario	Status de la Condición	Referencia de Evaluación
01/01/2005	Computador central AS-400	Jovita Guzmán / Ing.Julio Chang	No. Inventario DS-200	R/5 dado de baja el 01 enero 2009	©
01/01/2007	Computador central AS-400	Jovita Guzmán / Ing.Julio Chang	No. Inventario DS-400		©
01/01/2007	Firewall	Jovita Guzmán / Ing.Julio Chang	No. Inventario DS-411		©
01/01/2007	IPS (equipo de prevención de intrusos)	Jovita Guzmán / Ing.Julio Chang	No. Inventario DS-412		©
01/01/2007	Servidor de Red	Jovita Guzmán / Ing.Julio Chang	No. Inventario DS-400		©
01/01/2007	Servidor de Compensación	Jovita Guzmán / Ing.Julio Chang	No. Inventario DS-401		©
01/01/2007	Servidor de transacciones	Jovita Guzmán / Ing.Julio Chang	No. Inventario DS-402		©
01/01/2007	Servidor de Respaldo	Jovita Guzmán / Ing.Julio Chang	No. Inventario DS-405		©
01/01/2007	Servidor de Logistica	Jovita Guzmán / Ing.Julio Chang	No. Inventario DS-410		©
01/01/2007	Servidor de Internet y Correo	Jovita Guzmán / Ing.Julio Chang	No. Inventario DS-403		©
01/01/2007	Impresora multifuncional-canon	Jovita Guzmán / Ing.Julio Chang	No. Inventario DS-502		©
S/F	Servidor Marca IBM Serie 52-32251500			R/6 Equipo de prueba de terceros	©

Deficiencias encontradas

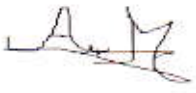
R/5 El computador central fue sustituido en fecha 01/01/2009 y dado de baja en libros de la contabilidad; sin embargo, aún permanece en el Departamento de Sistemas y la Administración no ha definido el uso que se dará al mismo en función de su estado actual.

R/6 El servidor corresponde a un equipo de prueba que pertenece a la empresa Servicampa, S.A y por ende no es de propiedad de Calzado Cobanera, S.A; este equipo ya se encuentra descontinuado en el mercado, y la administración no ha comunicado a la empresa proveedora el retiro del mismo y bajo qué condiciones.

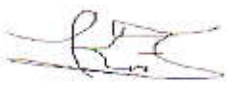
Conclusión y recomendación.

El 16% del total presentaron deficiencias, puesto que de doce (12) casos evaluados, dos (2) presentaron deficiencias porque: a) No se realizan inventarios físicos periódicos mediante los cuales puedan detectarse desviaciones importantes a los procedimientos y a las unidades existentes, b) La administración de la empresa no ha tomado decisión sobre el destino de los equipos obsoletos dados de baja y otros que no son de su propiedad, y, c) No se ha normado el uso que se debe dar a los equipos obsoletos por lo tanto afecta adversamente el espacio disponible del Departamento.

En consecuencia, y con el fin de evitar el riesgo de inversiones inadecuadas dadas por el registro y control de los equipos que ya se encuentran obsoletos y sin ningún uso de utilidad para la empresa, especialmente con los que no son de su propiedad, la Administración debe instruir al Gerente de Sistemas sobre lo procedente y además normar el procedimiento para casos futuros.



Ana Marilú Ávila
ENCARGADO EVALUACIÓN



Vo.Bo. Karin Figueroa
AUDITOR INTERNO

CALZADO COBANERO, S.A.

DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A9	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

REVISIÓN DEL INVENTARIO DE PROGRAMAS *(SOFTWARE)*

Se procedió a verificar y evaluar el inventario de *software* utilizados en la empresa se presenta en el siguiente cuadro.

Cantidad de Licencias	Identificación de los Programas	Versión actual	Cantidad Computadores autorizados	Cantidad computadores con Programas	Status de la Condición	Referencia de Evaluación
27	Windows	XP	27	27		⌂
25	Windows	2007	25	25		⌂
20	Office	2003	20	20		⌂
32	Office	2007	32	32		⌂
45	SPC	2009	45	45		⌂
4	Windows	2000	4	5	R/7 Sin licencia proveedor	⌂
1	Windows	98	1	1		⌂
7	Office	2000	7	7		⌂
52	Norton-32	2010	52	52		⌂

R/7 Solamente se encontró un caso en el que la empresa no posee licencia del proveedor para el uso de un programa actualmente instalado y funcionando.

Conclusión y recomendación.

Aunque en un caso aislado, el Departamento de Sistemas no ha aplicado como procedimiento, la comprobación de que todos los programas en uso *(Windows 2000* en el presente caso) estén apoyados por licencias del proveedor, originando riesgo de potenciales litigios posteriormente. A futuro y como procedimiento, el Gerente de Sistemas debe contar con un listado a mano con el que pueda estar

monitoreando constantemente todas las licencias que la empresa ha adquirido y en los equipos en donde está instalado el programa relacionado, así como la fecha de vigencia, asegurándose que no existen equipos con programas no controlados bajo ese listado.

Ana Marilú Ávila
ENCARGADO EVALUACIÓN

Vo.Bo. Karin Figueroa
AUDITOR INTERNO

CALZADO COBANERO, S.A.

DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A10	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

EVALUACIÓN DE LA CONFIABILIDAD DE LA INFORMACIÓN

Se procedió a verificar la confiabilidad de la información, en el cual se hizo una prueba selectiva. Los resultados se presentan a continuación.

Fecha de la Prueba Selectiva	Reportes de Información Financiera	Actividades de Evaluación y Resultados	Status de la Condición	Referencias de Evaluación
06/01/2010	Nómina de empleados área administrativa	Procesos verificados en elaboración de nomina y de los cálculos relacionados		✓ ⌂
07/01/2010	Planilla de empleados del área producción.	Procesos verificados en elaboración de planilla y de los cálculos relacionados		✓ ⌂
07/01/2010	Mayor de la cuenta de Proveedores	Comprobación satisfactoria con la integración del departamento de contabilidad, incluyendo la de saldos por antigüedad		✓ ⌂
08/01/2010	Reporte de la Facturación	Emisión de facturas manual, ingresando los movimientos generados al sistema al final del mes.	R/8 Reporte sin utilización	⌂
08/01/2010	Reporte del crédito Fiscal	Verificado el cálculo y cumplimiento del reporte y del % de impuesto con lo efectivamente enterado a la SAT.		✓ ⌂
08/01/2010	Ingreso de Liquidaciones de Anticipos	Error en la recepción de datos sobre cuenta contable en el Departamento de Contabilidad.	R/9 Error en asignación de cuenta y en recepción de contabilidad	ERR

Deficiencias encontradas

R/8Falta de utilización del reporte por parte del usuario

R/9 Error en la recepción del nombre y código de cuenta contable en contabilidad; no obstante que el usuario aplica la cuenta correcta, en el Departamento de contabilidad se recibe en una cuenta diferente.

Conclusión y recomendación.

De seis (6) casos evaluados, dos (2) presentaron diferentes fallas. La falta de utilización de ciertos reportes no contribuye con el usuario o empleado para el mejor desempeño de sus funciones, originando el riesgo de que los resultados de su gestión no sean los esperados. Por otra parte, no ha realizado una revisión del proceso de transferencia de datos, por lo cual el Departamento de Contabilidad tiene que realizar esfuerzos adicionales para la identificación de errores con el riesgo que en determinado momento no los detecte.

Por consiguiente, es necesario: a) Instruir a los usuarios de los sistemas de información para que hagan uso de ellos que los aprovechen tanto como sea posible, b) El Gerente de Sistemas y encargado de mantenimiento hagan una revisión exhaustiva de las causas que afectan a que la información procesada llegue al Departamento de contabilidad en forma correcta y oportuna; este tipo de debilidad es grave la cual debe tomarse acción inmediata.

Ana Marilú Ávila
ENCARGADO EVALUACIÓN

Vo.Bo. Karin Figueroa
AUDITOR INTERNO

CALZADO COBANERO, S.A.

DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A11	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

VERIFICACIÓN DEL INVENTARIO DE CINTAS DE RESPALDO *(BACK-UPS)* Y UBICACIÓN

Se procedió a verificar y evaluar el inventario de *back-up* de la información. El departamento de sistemas clasifican las cintas conforme al siguiente cuadro:

Fecha Back- Ups	Información Almacenada	Persona encargada de emitir la Copia	Persona que revisó	Referencia de Evaluación
15/09/2009	Archivo maestro de clientes	Mario Rivera	Marilú Ávila	Φ
23/09/2009	Archivo maestro de saldos al 06-10-2010	Juan Carlos Meza	Marilú Ávila	Φ
30/09/2009	Archivo de cierre parcial	Mario Rivera	Marilú Ávila	Φ
01/10/2009	Archivo maestro de operaciones en tiendas	Mario Rivera	Marilú Ávila	Φ
01/10/2009	Archivo maestro de la información Financiera	Juan Carlos Meza	Marilú Ávila	Φ
01/10/2009	Archivo maestro de la información Administrativa	Juan Carlos Meza	Marilú Ávila	Φ
31/12/2009	Archivo cierres anuales	Mario Rivera	Marilú Ávila	Φ

Conclusión y recomendación.

Se realiza y mantiene un procedimiento apropiado para la emisión de archivos de respaldo *(Back-Ups)*. Notamos que: a) Se emiten estos archivos con la información financiera y administrativa importante, b) Se realiza la emisión de estos archivos con una periodicidad aceptable (diarios, parciales y anuales). En conclusión, no se establecieron desviaciones importantes para su divulgación. Solamente recomendamos que se mantenga la consistencia de los procedimientos y que el Gerente de Sistemas continúe monitoreando estos aspectos del procedimiento.

Ana Marilú Ávila
ENCARGADO EVALUACIÓN

Vo.Bo. Karin Figueroa
AUDITOR INTERNO

CALZADO COBANERO, S.A.

DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A12	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

EVALUACIÓN DE LA SEGURIDAD FÍSICA DE LAS INSTALACIONES DEL DEPARTAMENTO DE SISTEMAS.

Conforme plan de trabajo se procedió a verificar los equipos utilizados para proporcionar la seguridad física, a las instalaciones del departamento de sistemas (D.S), los resultados fueron los siguientes:

Fecha de revisión del encargado en Mantenimiento	Identificación del Equipo	Comentarios sobre su ubicación y funcionamiento	Status de la Condición	Referencia de Evaluación
03/01/2008	Alarmas detectoras de humo	Se cuenta con 2 alarmas detectoras de humo distribuidas adecuadamente. No se ha revisado las cargas en el último año como lo indica el fabricante.	R/10 Falta carga Anual	B ⌂
25/10/2008	Extintores de incendios	Existen 4 extintores distribuidos adecuadamente, pero que no se ha revisado las cargas en el último año como lo indica el fabricante.	R/10 Falta carga anual	B ⌂
30/09/2009	Cámara de vigilancia	Existen cámaras distribuidas de la siguiente manera: al ingreso al D.S, monitoreando al operador de turno y el ingreso a los servidores. Todas funcionando a satisfacción.		B
31/12/2009	Aire Acondicionado	El aire acondicionado funciona adecuadamente.		B
02/01/2010	Dispositivo para evitar inundaciones	Los equipos están instalados a 25 cc del suelo y se cuenta con un dispositivo que absorbe a su interior el agua proveniente de inundaciones. Funcionando apropiadamente.		B
10/01/2010	Alarmas detectoras de temperatura y de humedad	Para mantener la temperatura en 17 grados centigrados y prevenir daños ocasionados por humedad se cuenta con 2 alarmas detectoras funcionando adecuadamente.		B
18/01/2010	Equipos y Programas (hardware y Software) para control de ingreso al Departamento de Sistemas.	Para el ingreso al D.I se utiliza una tarjeta y un código personalizado; el registro de estos ingresos es hecho automáticamente y se puede consultar de manera cronológica. Funcionando a satisfacción.		B
20/01/2010	Reguladores de voltaje y UPS	Los equipos están protegidos con un regulador de voltaje y un UPS capaz de mantener el servicio solo por 1/2 hora.	R/11 Capacidad funcionamiento solo por media hora	B

Deficiencia establecida

R/10Conforme a las especificaciones del fabricante, la carga de los extintores de incendios y de los detectores de humo, deben ser revisados una vez al año; para el último año, esta revisión no ha sido hecha por el encargado en mantenimiento.

R/11El equipo de UPS, solamente está funcionando parcialmente ya que presenta capacidad de mantener el servicio solo por ½ hora.

Conclusión y recomendación.

Se recomienda establecer un procedimiento escrito, en el cual se contemple la periodicidad necesaria para el mantenimiento de los equipos, ya que no estaríamos preparados para un siniestro, es necesario llevar el control de dichos extintores de incendios y de las alarmas detectoras de humo.

Se determino que el UPS con el que cuentan para mantener el servicio solamente es capaz de resistir ½ hora, por lo que recomendamos que se evalúen otros UPS con los que se cuente con mayor resistencia.

Ana Marilú Ávila
ENCARGADO EVALUACIÓN

Vo.Bo. Karin Figueroa
AUDITOR INTERNO

CALZADO COBANERO, S.A.

DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A13	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

REVISIÓN DE LOS CONTRATOS DE MANTENIMIENTO DE EQUIPOS DEL DEPARTAMENTO DE SISTEMAS.

Conforme al plan de trabajo se procedió a verificar los contratos de mantenimientos de equipos del departamento de sistemas, los resultados se presentan a continuación.

Fecha de Vencimiento	Identificación del Contrato	Empresa Contratista	Situación actual del Contrato	Status de la Condición	Referencia de Evaluación
01/12/2008	Mantenimiento del aire acondicionado.	AIRES, S.A.	A la fecha aún no se ha renovado el contrato	R/12 Falta renovación contrato	µ ⌂
01/12/2009	Mantenimiento del equipo de cómputo.	SERVICAMPA, S.A.	El contrato está vigente y cubre adecuadamente el mantenimiento preventivo y correctivo de los equipos. Las cuotas se mantienen pagadas al día.		µ ⌂
02/01/2010	Mantenimiento del equipo UPS.	TELGUEX, S.A	El contrato ha sido aplicado en dos ocasiones por desperfectos en el equipo. Las cuotas se mantienen pagadas al día.		µ ⌂
31/10/2010	Mantenimiento del equipo de telecomunicaciones.	TELGUEX, S.A	El mantenimiento se realiza trimestralmente tal y como se establece en el contrato. Las cuotas se mantienen pagadas al día.		µ ⌂
31/12/2010	Mantenimiento del cableado.	TELGUEX, S.A	Se emiten boletas de servicio mensuales. Las cuotas se mantienen pagadas al día.		µ ⌂

Deficiencia establecida

R/12Un caso presenta falla de no haberse renovado el contrato correspondiente.

Conclusión y recomendación.

Uno (1) caso de los cinco (5) que fueron revisados y evaluados, presentó deficiencia en cuanto a no haberse renovado el contrato de mantenimiento, originando un riesgo potencial de que el proveedor en determinado momento no preste el servicio, interrumpiendo las operaciones relacionadas. Con ello, la falta de un procedimiento escrito que promueva el conocimiento constante sobre la negociación y control de los contratos de mantenimiento.

En consecuencia, es muy importante que se incorpore un registro con todos los datos de los contratos de mantenimiento, para que el encargado pueda todos los meses verificar su vigencia o la necesidad de su renovación, informando de todo a la Gerencia General para la toma de decisiones.

Ana Marilú Ávila
ENCARGADO EVALUACIÓN

Vo.Bo. Karin Figueroa
AUDITOR INTERNO

CALZADO COBANERO, S.A.

DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A14	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

REVISIÓN DE LAS POLIZAS Y DE LOS CONTRATOS DE SEGURO

Se procedió a verificar los contratos de seguros de equipos, del departamento de sistemas, los resultados se presentan a continuación:

Fecha de Vencimiento de la Póliza	Tipo de Seguro	Aseguradora	Situación actual del contrato y póliza	Status de la condición	Referencia de Evaluación
01/05/2009	De Responsabilidad Civil, de accidentes en el área del Departamento de sistemas	La Seguridad Eficaz, S.A.	A la fecha aún no se ha renovado contrato.	**R/12 Falta de renovación contrato**	⌂
31/12/2009	De reposición Equipo de cómputo en caso de incendios, inundaciones y robo	La Seguridad Eficaz S.A.	En vigencia y mantiene el pago de las cuotas hasta el año 2009.		µ ⌂

Deficiencia establecida

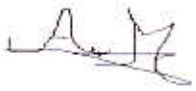
R/12Un caso presenta falla de no haberse renovado el contrato correspondiente.

Conclusión y recomendación.

Uno (1) caso de los dos (2) que fueron revisados y evaluados, presentó deficiencia en cuanto a no haberse renovado el contrato de mantenimiento, originando un riesgo potencial de que el proveedor en determinado momento no preste el servicio, interrumpiendo las operaciones relacionadas. Con ello, la falta de un

procedimiento escrito que promueva el conocimiento constante sobre la negociación y control de los contratos de mantenimiento.

En consecuencia, es muy importante que se incorpore un registro con todos los datos de los contratos de mantenimiento, para que el encargado pueda todos los meses verificar su vigencia o la necesidad de su renovación, informando de todo a la Gerencia General para la toma de decisiones.



Ana Marilú Ávila
ENCARGADO EVALUACIÓN

Vo.Bo. Karin Figueroa
AUDITOR INTERNO

CALZADO COBANERO, S.A.

DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A15	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

VERIFICACIÓN DE LA SEGURIDAD DE LA TECNOLOGÍA INFORMÁTICA

Conforme al plan de trabajo se procedió a verificar la seguridad de la tecnología informática, los resultados se presentan a continuación.

Fecha de la Evaluación y Verificación de Auditoria	Programa en aplicación	Situación Actual de la Condición	Referencia de Evaluación
16/01/2010	Firewall	Este dispositivo funciona como corta-fuegos entre redes, permitiendo o denegando las transmisiones de una red a otra y es utilizado en una red local y una red de internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial	®
16/01/2010	Antivirus Spaware	Este antivirus viene incorporado en el correo, en el cual está configurado para bloquear los archivos infectados	®
16/01/2010	Antivirus Norton-32	Este antivirus está instalado en los equipos y es utilizado y actualizado automáticamente.	®

Conclusión y recomendación.

Aunque las evaluaciones fueron satisfactorias, es importante que se mantenga en forma consistente el proceso de actualización, puesto que estos programas cambian con una regularidad constante y son obsoletos en un corto período de tiempo. Sin embargo, el Departamento de Sistemas se ha preocupado por la actualización constante lo cual es una fortaleza para el área de seguridad.

Ana Marilú Ávila
ENCARGADO EVALUACIÓN

Vo.Bo. Karin Figueroa
AUDITOR INTERNO

CALZADO COBANERO, S.A.

DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A16	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

VERIFICACIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO (PCN)

Se procedió a verificar el plan de continuidad del negocio, los resultados se presentan a continuación.

Número orden.	Proceso	Status de la condición	Referencia de Evaluación
1	Copia del Plan vigente de la continuidad del negocio (PCN)	La copia obtenida, ha sido actualizada al 20/12/2009	⌂
2	Muestras de copias distribuidas del PCN	Se distribuyeron dos (2) copias al personal involucrado en el PCN	≠
3	Inventario de actividades y procesos críticos	El Plan identifica los procesos criticos que se incluyen en la matriz diseñada para el efecto, misma que esta adjunta al PCN.	¥
4	Listado de proveedores y clientes a informar con relación a la contingencia	Se enviaron notas de actualización de los aspectos necesarios	≠
5	Determinación de prioridades en cuanto a la restauración de operaciones	En el Plan se ordenan las actividades y se asignan prioridades	≠
6	Lugar o sitio alterno para el procesamiento de información	El Plan determina el sitio alterno, por una interface se realizaría automáticamente la réplica de todas las operaciones del sistema principal	≠
7	Personal encargado de ejecutar el PCN	En el Plan se describen los números telefónicos del personal encargado de ejecutarlo	£
8	Conocimiento del personal del PCN	Selectivamente fue seleccionado el personal notando que cuentan con los conocimientos suficientes para ejecutar en determinado momento el PCN	≠
9	Actualización del PCN	Se comprobó que el Plan es actualizado por lo menos dos veces al año y que consigna las fechas de actualización; se analizaron actualizaciones de los últimos dos años.	≠
10	Pruebas al PCN	Para verificar la funcionalidad del PCN se ha establecido la realización de una prueba en el año, anotando la fecha y resultados de esta. Se obtuvo evidencia de la última prueba en el año 2,009	✓

Conclusión y recomendación.

La evaluación reveló la tenencia de un apropiado Plan de Continuidad del Negocio y que el mismo se actualiza dos veces al año, lo cual consideramos es aceptable. La administración se preocupa porque el PCN se encuentre siempre disponible y que el personal esté constantemente recibiendo los conocimientos del mismo y de los cambios o modificaciones que se generan en cada año. Solamente recomendamos que el Plan siga siendo objeto de actualización y aprobación año con año.

Ana Marilú Ávila
ENCARGADO EVALUACIÓN

Vo.Bo. Karin Figueroa
AUDITOR INTERNO

CALZADO COBANERO, S.A.

DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A17	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

MATRIZ DE RIESGOS ASOCIADOS A LOS HALLAZGOS ESTABLECIDOS

La Matriz de Riesgos es una orientación visual que en forma sencilla otorga prioridades en la atención de determinados riesgos.

Con el fin de dar a conocer a la Administración de la empresa Calzado Cobanero, S.A., los niveles de Riesgo asociados a cada uno de los hallazgos o deficiencias establecidos con la Evaluación del Control Interno Informático en el área de Seguridad en el Departamento de Sistemas, así como el impacto en las operaciones de la empresa y principalmente en cuanto a las Oportunidades de Mejora (como opciones de fortalecimiento y de eliminación de las causas y origen de deficiencias), fue elaborada una Matriz conteniendo una amplia descripción de todos esos asuntos.

Esta Matriz, fue debidamente presentada al Gerente de Sistemas para obtener sus comentarios y observaciones de cada caso con el fin de hacer las incorporaciones o cambios que fueron aplicables. En este sentido, constituye la base fundamental del Informe de Auditoría emitido, su contenido constituye un valioso aporte a la Administración para la toma de sus decisiones.

Para una mejor comprensión, en esta Matriz que se presenta se hace uso de ciertos colores que representan principalmente los niveles de riesgo asociados, de la siguiente forma: a) El color verde representa un nivel Bajo Riesgo, b) El color amarillo representa un nivel medio de Riesgo, y, c) El color rojo representa un nivel alto de Riesgo.

EVALUACIÓN DE PROCESOS RELEVANTES

CALZADO COBANERA, S.A.

MATRIZ DE RIESGO

PROCESO: AREA DE SISTEMAS

Fecha de Evaluación: Enero 2010

Clasificación de Riesgos: (I) RIESGO INHERENTE, (C) RIESGO CONTROL, (D) RIESGO DETECCION.

#	Riesgo	OPORTUNIDAD DE MEJORA	CAUSA	EFECTO (posible)	Riesgos				RECOMENDACIÓN
					Control	Inherente	Detección	Riesgo	
1	Clave y acceso del personal de sistemas que ingresaron sin autorización.	Es posible aprovechar la existencia y uso de los formularios debidamente diseñados, aprobados y establecidos para evitar ingresos no autorizados del personal ajeno al Departamento de Sistemas	Falta de exigencia del encargado para que la persona presente el formulario debidamente firmado por el funcionario designado o en su defecto no permitir la entrada.	Potenciales pérdidas de equipo (hardware) y de intervenciones adversas en los programas (software) y por consiguiente potencial pérdida de valiosa información operativa, administrativa y financiera.	X	X	X	G	El encargado en el Departamento de Sistemas debe solicitar invariablemente el formulario autorizado para el respectivo ingreso. Por ello, es de suma importancia instruir nuevamente al encargado sobre su responsabilidad de solicitar a toda persona, sin distinción alguna, la autorización para el acceso al Departamento de Sistemas.
2	Clave del personal de sistemas que no han sido cambiadas con periodicidad.	La empresa y el Departamento de Sistemas tiene la opción de aprovechar los procedimientos ya aprobados para realizar aquellos cambios a sus claves de acceso conforme la periodicidad que ha sido establecida .	a) Se determino que el Gerente de Sistemas no estaba sujeto al cambio periódico de su clave de acceso por ser la autoridad superior, b) la falta de validación constante y de la actualización de claves originaron la debilidad de acceso no autorizado por el personal del Departamento.	Potenciales pérdidas de equipo (hardware) y de intervenciones en los programas (software) y por consiguiente potencial pérdida de valiosa información operativa, administrativa y financiera	X		X	M	Las claves de acceso del señor Gerente de Sistemas sean actualizadas como lo requiere el procedimiento establecido y aprobado.

#	Riesgo	OPORTUNIDAD DE MEJORA	CAUSA	EFECTO (posible)	Riesgos				RECOMENDACIÓN
					Control	Inherente	Detección	Riesgo	
3	Inventario de Equipos (Hardware) que ingresan al Departamento de Sistemas por reparaciones	El diseño de un Procedimiento que norme la obligatoriedad de presentar con cada retiro de equipo del departamento de sistemas: a) Formulario con la fecha de ingreso y de devolución b) Informe de diagnostico de la condición del equipo que justifique su salida, c) Informe final de la reparación.	a) Falta de iniciativa del encargado de requerir algunos documentos para el control, o de dar aviso inmediato de la ocurrencia del caso, y, b) Falta de asignación de responsabilidad a un funcionario para el diseño del procedimiento.	Perdida de equipo.	X	X	X	G	a) Realizar un diagnóstico y diseño del procedimiento para realizar todos los cambios y mejoras al mismo, b) Instruir inmediatamente al encargado para que no permita el retiro del equipo sin documentos de registro y control.
4	Inventario de Equipos (Hardware) del Departamento de Sistemas.	La empresa puede normar a la brevedad el procedimiento de realizar inventarios e inspecciones fisicas periódicas, al menos 2 veces por año.	Se confia únicamente en que los equipos se encuentren físicamente, pero no se advierte sobre potenciales situaciones de obsolescencia y de utilización de equipo ajeno.	a) Gasto de recursos de la empresa para mantener controles de equipos que no lo ameritan, y su costo de almacenamiento, b) Potenciales reclamos de la empresa proveedora del equipo	X		X	M	Realización de inventarios periódicos (cada 6 meses) que enfaticen sobre la obsolescencia, inutilización, y existencia de equipos ajenos.
5	Inventario de programas (Software)	La empresa a la fecha, puede adquirir la licencia para uso del programa Windows 2000 en uso.	Ocurrencia de un empleado en la instalación del programa sin percatarse de la ausencia de la licencia.	Potenciales litigios con el proveedor de las licencias.	X			L	El gerente de sistemas debe contar con un listado mediante al cual pueda monitorear constantemente las licencias que la empresa a adquirido y los equipos de los programas que están instalados..

#	Riesgo	OPORTUNIDAD DE MEJORA	CAUSA	EFECTO (posible)	Riesgos				RECOMENDACIÓN
					Control	Inherente	Detección	Riesgo	
6	Confiabilidad de la Información	Es factible: a) Instruir al encargado en el ingreso de los movimientos de facturación al sistema en forma diaria, b) Solicitar al Ing. Julio Chang (Gerente de Sistemas) un informe de error de proceso de la cuenta contable. .	a) Falta de instrucciones al encargado para la operación diaria, y, b) Ninguna intervención del Departamento de sistemas para la detección de errores en el proceso de digitación de cuentas y la razonabilidad de aplicación a la contabilidad.	a) Bajo desempeño del encargado e información inoportuna en el sistema, y , b) Posibilidad de que errores e irregularidades puedan ocurrir y no sean detectadas en forma oportuna.	X	X	X	G	a) Instruir a los usuarios de los sistemas de información para que hagan uso de ellos y los aprovechen tanto como sea posible, y, b) El Gerente de Sistemas y encargado de mantenimiento del programa, hagan una revisión exhaustiva de las causas que afectan a que la información procesada llegue al Departamento de contabilidad en forma incorrecta inoportuna
7	Seguridad fisica.	a) La empresa debe normar un procedimiento para realizar el mantenimiento de los equipos, b) La compra de UPS con mayor resistencia.	a) Se confian y no se percatan que efectivamente se estén realizando los mantenimientos a los equipos, y, b) Ninguna intervención del Departamento de Sistemas para evaluar la resistencia de los UPS.	a) Perdida de equipo por alguna catástrofe que surja en el futuro, y, b) Perdida de información.	X	X	X	G	a) Establecer un procedimiento escrito, en el cual se contemple la periodicidad necesaria para el mantenimiento de los equipos, ya que no estaríamos preparados para un siniestro, es necesario llevar el control de dichos extintores de incendios y de las alarmas detectoras de humo, y, b) evaluar otros UPS con los que se cuente con mayor resistencia.

#	Riesgo	OPORTUNIDAD DE MEJORA	CAUSA	EFECTO (posible)	Riesgos				RECOMENDACIÓN
					Control	Inherente	Detección	Riesgo	
8	Seguridad en los Contratos de Seguros.	La empresa puede normar a la brevedad el procedimiento y control de los contratos de mantenimiento y seguros.	Se confían en los proveedores. Por lo consiguiente no efectúan las renovaciones correspondientes.	a) Potenciales perdidas al momento que surja un siniestro, b) Las reparaciones sean con mayor inversión.	X	X		G	Que se incorpore un registro con todos los datos de los contratos de mantenimiento, para que el encargado pueda todos los meses verificar su vigencia o la necesidad de su renovación, informando de todo a la Gerencia General para la toma de decisiones.

Leve	1
Moderado	2
Grave	5
Total···	8

CALZADO COBANERO, S.A.

DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A18	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

PLAN DE ACCIÓN PARA MEJORAS DE LOS RIESGOS DETECTADOS

Plan de Acción			
No.	Riesgo	Actividad y Responsable	Fecha
1	Clave y acceso del personal de sistemas que ingresaron sin autorización.	A partir de la fecha y al final de cada dia, el Ing. Julio Chang verificará que la copia de los formularios de ingreso presenten la firma de autorización	02/02/2010
2	Clave del personal de sistemas que no han sido cambiadas con periodicidad.	Las correcciones ya fueron hechas por el Ing. Julio Chang, quien a partir de la fecha verificará la actualización conforme las fechas indicadas según el procedimiento.	31/01/2010
3	Inventario de Equipos (Hardware) que ingresan al Departamento de Sistemas por reparaciones.	Gerencia General asignará la función de diagnóstico y diseño al Ing. Julio Chang y, este a su vez a dado las instrucciones de caso al encargado.	15/02/2010
4	Inventario de Equipos (Hardware) del Departamento de Sistemas.	El Ing. Julio Chang y el personal del Departamento procederán a realizar estos inventarios, de forma inmediata.	02/02/2010
5	Inventario de programas (Software)	El Ing. Julio Chang procederá inmediatamente a realizar el monitorio y seguimiento correspondiente.	02/02/2010
6	Confiabilidad de la Información	a) Gerencia General emitirá instrucciones escritas para que el jefe de área instruya a su personal, y, b) El Ing. Julio Chang juntamente con el Contador General procederá inmediatamente a realizar el estudio.	02/02/2010
7	Seguridad fisica.	El Ing. Julio Chang procederá inmediatamente a realizar el monitorio y seguimiento correspondiente.	31/01/2010
8	Seguridad en los Contratos de Seguros.	El Ing. Julio Chang procederá inmediatamente a realizar el monitorio y seguimiento correspondiente.	31/01/2010

Ana Marilú Ávila
ENCARGADO EVALUACIÓN

Vo.Bo. Karin Figueroa
AUDITOR INTERNO

4.2.4 Informe de la Evaluación del Control Interno Informático sobre el área de Seguridad del Departamento de Sistemas.

CALZADO COBANERO, S.A.
DEPARTAMENTO DE AUDITORÍA INTERNA.

P.T. No.		A19	
Hecho Por:	M.A.O	Fecha:	01/01/2010
Revisado Por:	K.F.C	Fecha:	29/01/2010

Guatemala, 29 de enero 2010

Licenciado Estuardo Flores

Gerente General

Calzado Cobanero, S.A

Señor Gerente:

Este informe presenta los resultados de la Evaluación del Control Interno Informático en el área de Seguridad del Departamento de Sistemas de la empresa, realizada a fecha 29 de enero 2010. El contenido del mismo fue ampliamente discutido con el señor Gerente de Sistemas en fecha 27 de enero 2010 habiéndose incorporado al mismo sus comentarios y puntos de vista que consideramos fueron aplicables.

ASPECTOS EVALUADOS

1. Se verifico la propiedad de la seguridad y protección de la información, del sistema computacional, de los recursos informáticos de la empresa y el cumplimiento de los planes, programas, estándares, políticas, normas y lineamientos que regulan las funciones y actividades de seguridad en las

áreas y sistemas de procesamiento de información, así como del personal y de los usuarios del centro de información.

2. Se evaluó si los sistemas y procedimientos proporcionan la integridad, confiabilidad de la información, seguridad del personal, los datos, equipos (*hardware*), programas (*software*) e instalaciones, y la apropiada custodia de los activos para asegurar la inexistencia de usos no autorizados y de la disposición ilegal de los mismos.

3. Se verifico el plan de continuidad del negocio, la seguridad en las instalaciones mantenimientos y seguros.

OBSERVACIONES DE AUDITORÍA

Derivado de la revisión de los procedimientos y normativa interna y tomando en consideración la matriz de impacto de riesgos detectados, se obtuvieron las siguientes conclusiones:

Riesgo Leve

1. La revisión del inventario de programas *(Software),* se detecto en un caso que no posee licencia del proveedor para el uso de un programa actualmente instalado y funcionando.

Riesgo Moderado

2. En las claves de acceso requeridas para el ingreso del personal al Departamento de sistemas, se detecto que deben hacer los cambios de claves periódicamente como lo tienen establecido en el procedimiento aprobado.

3. En la revisión del inventario de equipos de cómputo en el Departamento de Sistemas, se detectaron deficiencias porque no realizan inventarios físicos periódicos, y la administración no ha tomado la decisión sobre el destino de equipos obsoletos.

Riesgo Grave

4. Se estableció en el control de Acceso del personal externo al Departamento de no cumple con los procedimientos aprobados y establecidos en cuanto a la autorización del ingreso al personal externo; hubo falta de requerimiento por parte del encargado.

5. Se estableció en la evaluación de control del egreso de equipo del Departamento de Sistemas no se cuenta registro de la fecha de ingreso y devolución, un diagnostico que justifique la salida del equipo.

6. Se estableció en la evaluación de la confiabilidad de la información, falta de instrucciones al encargado para la operación diaria a la persona encargada de facturación por parte del Departamento de Sistemas y se encontraron errores en la recepción el ingreso de liquidaciones de anticipos.

7. En la seguridad física de las instalaciones del Departamento de Sistemas, se detecto que no hay un procedimiento para realizar mantenimiento a los equipos, la carga de los extintores de incendios y de los detectores de humo no han sido revisados, el equipo de UPS se determino que solamente está funcionando parcialmente ya que presenta un capacidad minima de servicio.

8. En la revisión de los contratos de mantenimiento y seguros se determino que no existe un procedimiento escrito para la negociación y control de los contratos, se encuentran vencidos ciertos contratos y que aun no han sido renovados.

RECOMENDACIONES

1. El gerente de sistemas debe contar con un listado mediante al cual pueda monitorear constantemente las licencias que la empres a adquirido y los equipos de los programas que están instalados.

2. Las claves de acceso del Gerente de Sistemas sean actualizadas como lo requiere el procedimiento establecido y aprobado.

3. Es conveniente la realización de inventarios periódicos a efecto de verificar la existencia física de los equipos en el Departamento de Sistemas. Así como traslado de equipo obsoleto y existencia de equipos ajenos al departamento.

4. El encargado del Departamento de Sistemas debe solicitar invariablemente el formulario autorizado para el respectivo ingreso al acceso al Departamento.

5. Se sugiere realizar un diagnostico y diseño del procedimiento, e instruir inmediatamente al encargado para que no permita el retiro del equipo sin documentos de registro y control.

6. Instruir a los usuarios de los sistemas de información para que hagan uso de ellos y los aprovechen tanto como sea posible.

   El gerente de sistemas y el encargado de mantenimiento del programa, hagan una revisión exhaustiva de las causas que afectan a que la información procesada llegue al Departamento de contabilidad en forma incorrecta inoportuna.

7. Establecer un procedimiento escrito, en el cual se contemple la periodicidad necesaria para el mantenimiento de los equipos, es necesario llevar el control de los extintores de incendios y de las alarmas detectoras de humo. Evaluar otros UPS con lo que se cuente con mayor resistencia.

8. Que se incorpore un registro con todos los datos de los contratos de mantenimiento, para que el encargado pueda verificar su renovación, informando de todo a la Gerencia General para la toma de decisiones.

COMENTARIOS DEL AUDITADO

Los riesgos y recomendaciones fueron discutidos y aprobados con el Gerente de Sistemas. La decisión del señor Gerente fue la de iniciar con mucha disposición la puesta en práctica de algunas Recomendaciones aplicables y que a nuestro juicio son posibles, por las cuales estará emitiendo en los próximos cinco días un informe a Gerencia General y copia a esta Auditoría Interna.

Cualquier duda en relación al contenido de este Informe, favor de emitir instrucciones para aclaración o ampliación inmediata.

Atentamente,

Karin Figueroa
AUDITOR INTERNO

CONCLUSIONES

1. En la actualidad la actividad industrial del calzado es de gran importancia para la economía nacional y constituye una fuente importante de empleo para la población guatemalteca, tanto para las personas que laboran en las empresas proveedoras de materias primas, como para aquellas que forman parte de las empresas distribuidoras de producto terminado al consumidor final. El desarrollo de esta actividad se presentó entre los años de 1,940 a 1,950 en donde además de las industrias de calzado de piel, se constituyeron en Guatemala fábricas dedicadas a producir calzado deportivo y de hule; en consecuencia, la producción se diversificó y se promovió un avance tecnológico para la fabricación de los productos, dando lugar a un crecimiento importante a nivel de esta industria.

2. Es de vital importancia que se realice una Auditoría de sistemas en una industria de calzado ya que permite identificar y evaluar los diferentes procedimientos e informes, así como identificar sus principales riesgos y tomar las acciones adecuadas para el resguardo y uso de la tecnología.

3. El Control Interno Informático, comprende el Plan de Organización de todos los procedimientos coordinados de manera coherente, atinentes a las necesidades de la empresa y al cumpliendo de requerimientos legales. El mismo ha cobrado mucha importancia en los últimos años, ya que su correcta aplicación conduce a conocer la situación real de la empresa, con el propósito de salvaguardar los activos de la misma y de mantener la integridad de los datos utilizando eficientemente los recursos con que cuenta. Permite realizar planes de contingencias, dictar normas de seguridad informática, controla la calidad de software, los costos, control de licencias, manejo de claves de cifrado, es claro que esta medida permite la seguridad informática.

4. El informe COSO ERM (Gestión de Riesgo Empresarial) proporciona una normativa mediante la cual las empresas, independientemente de su tamaño, pueden evaluar su sistema de control y determinar su mejoramiento. Es actualmente una herramienta utilizada para obtener la comprensión del control interno existente en una empresa, lo cual ayuda al Contador Público y Auditor a planear procedimientos sustantivos de auditoría y a proporcionar observaciones y recomendaciones constructivas sobre cómo podría mejorar la administración.

5. Con la investigación se comprobó la hipótesis planteada referente a las deficiencias que pueden existir en una industria de calzado, por no evaluar apropiadamente el Control Interno Informático en el área de Seguridad de Sistemas.

RECOMENDACIONES

1. Los propietarios de las empresas industriales de calzado deben tomar en cuenta que es necesario evaluar periódicamente el control interno informático, con el propósito de que se tomen a tiempo las acciones preventivas y correctivas que se consideren necesarias.

2. Que el departamento de auditoría interna de una industria de calzado realice evaluaciones al Departamento de Sistemas, para identificar oportunamente riesgos y debilidades de control interno, comunicando a través de sus informes las recomendaciones que se consideren ayudaran a solventar los problemas detectados.

3. El uso del control interno informático en las organizaciones, como herramienta útil para la toma de decisiones, debe ser aplicado adecuadamente por parte de los propietarios y administradores, caracterizado por una actitud responsable, comprometida y bajo políticas de constante actualización, para el adecuado cumplimiento de los objetivos empresariales, eficiencia, productividad y custodia en la información.

4. Los empresarios que observen y apliquen las referencias incluidas en el informe COSO ERM (Gestión de Riesgo Empresarial), tienen la oportunidad de administrar y contrarrestar el efecto de riesgos que impiden el crecimiento y la consecución de objetivos de las entidades. El Contador Público y Auditor la utilización del COSO ERM en sus auditorías busque aportar observaciones y recomendaciones constructivas para las entidades donde labore o preste sus servicios.

5. Que derivado a la evaluación del control interno informático sobre la seguridad del área de sistemas, se considera oportuno que la administración y la auditoría interna, se capacite constantemente en las mejores prácticas para la gestión y administración de esta, para garantizar oportunamente los cambios y minimizar los riesgos que surjan.

BIBLIOGRAFÍA

1. Boletín 5030. Comisión de Normas y Procedimientos de Auditoría del Instituto Mexicano de Contadores Públicos.

2. Borges, Jorge Luis DICCIONARIO ENCICLOPÉDICO GRIJALBO. Aragó, 385, Barcelona, España, Nueva Edición, 1,995, 2,064 Páginas.

3. Cepeda Alonso, Gustavo "Auditoría y Control Interno", editorial Mcgraw Hill, Colombia 2000.

4. COMMITTE of Sponsoring Organizations of the Treadway Commission (COSO). Gestión de Riesgos Corporativos – Marco Integrado Técnicas de Aplicación. PricewaterhouseCoopers. Estados Unidos 2005. 125p.

5. Echevenique García, José Antonio. AUDITORIA EN INFORMATICA, México, 2001. Editores, S.A de C.V 2da. Edición, Paginas 299

6. Hernández Sincal, Felipe, Hernández Prado, Carlos Humberto. CURSO DE FINANZAS III, Guatemala, 2006. Páginas 160

7. Muñoz Razo, Carlos. AUDITORIA EN SISTEMAS COMPUTACIONALES, México, 2002. Editorial Pearson Educación. Páginas 816

8. Objetivos de Control para la Información y Tecnologías Afines COBIT Instituto de Gobierno de Tecnología de Información Estados Unidos de América. 2002.

9. Secretaría de Economía del Gobierno de México. Guía de Calzado. Disponible en red en:
Web: http://contactopyme.gob.mx/guiasesmpresariales. 211 Páginas.

10. Universidad San Carlos de Guatemala, Luis Lopez. Tesis El Valor Económico Agregado (EVA) en una Empresa Industrial de Calzado Sintético 2008, Paginas 124.

11. Web: http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

12. Web: http://www.coso.org

13. Web: http://www.revistaindustria.com TRAS LOS PASOS DEL CONSUMIDOR MODERNO

14. Web: www.itson.mx/dii/epadilla/areas.doc Auditoria de Sistemas de Información, Páginas (1-15)

15. Web: www.monografias.com/trabajos59/evolucion-control-interno/evolucion-control-interno.shtml

16. Web: www.theiia.org Normas Internacionales Para el Ejercicio Profesional de la Auditoría Interna, Páginas (1-22)