

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS

**“EL PAPEL DEL CONTADOR PÚBLICO Y AUDITOR, COMO AUDITOR
INTERNO EN LA ELABORACIÓN DE PROCEDIMIENTOS DE CONTROL
INTERNO EN LA PREVENCIÓN DE FRAUDES INFORMÁTICOS EN EL
ÁREA DE CUENTAS POR COBRAR PARA UNA EMPRESA DE
TRANSPORTE TERRESTRE”**



PREVIO A CONFERÍRSELE EL TÍTULO DE

CONTADOR PÚBLICO Y AUDITOR

EN EL GRADO ACADÉMICO DE

LICENCIADO

Guatemala, octubre de 2015

**MIEMBROS DE LA JUNTA DIRECTIVA
FACULTAD DE CIENCIAS ECONÓMICAS**

Decano:	Lic. Luis Antonio Suárez Roldán
Secretario:	Lic. Carlos Roberto Cabrera Morales
Vocal Segundo:	Lic. Carlos Alberto Hernández Gálvez
Vocal Tercero:	Lic. Juan Antonio Gómez Monterroso
Vocal Cuarto:	P.C. Oliver Augusto Carrera Leal
Vocal Quinto:	P.C. Walter Obdulio Chigüichón Boror

**PROFESIONALES QUE REALIZARON LOS EXÁMENES
DE ÁREAS PRÁCTICAS BÁSICAS**

Área Matemática-Estadística	Lic. Felipe Hernández Sincal
Área Contabilidad	Lic. Erik Roberto Flores López
Área Auditoría	Lic. M.Sc. Álvaro Joel Girón Barahona

**PROFESIONALES QUE REALIZARON EL
EXAMEN PRIVADO DE TESIS**

Presidente	Lic. Felipe Hernández Sincal
Secretario	Lic. Jorge Luis Reina Pineda
Examinador	Lic. Mario Leonel Perdomo Salguero

Guatemala, mayo de 2014.

Lic. José Rolando Secaida Morales
Decano de la Facultad de Ciencias Económicas
Universidad de San Carlos de Guatemala
Ciudad Universitaria zona 12
Ciudad.

Señor Decano:

De conformidad con la designación que me hiciera en su oportunidad la decanatura a su cargo, contenido en el oficio **DIC.AUD.311-2013** de fecha 12 de septiembre del año 2013, procedí a asesorar el trabajo de Tesis titulado **“EL PAPEL DEL CONTADOR PÚBLICO Y AUDITOR, COMO AUDITOR INTERNO EN LA ELABORACIÓN DE PROCEDIMIENTOS DE CONTROL INTERNO EN LA PREVENCIÓN DE FRAUDES INFORMÁTICOS EN EL ÁREA DE CUENTAS POR COBRAR PARA UNA EMPRESA DE TRANSPORTE TERRESTRE”** preparado y presentado por el señor **ADRIAN PINEDA GARCÍA** estudiante de la Facultad de Ciencias Económicas de esa casa de estudios superiores.

El Trabajo que presenta el señor Pineda, está desarrollado en forma ordenada y revela el resultado de la investigación efectuada en los ámbitos de transporte, de informática y auditoría interna. Por lo que considero ha sido elaborado satisfactoriamente, atendiendo los requisitos académicos exigidos por la facultad bajo su administración.

Consecuentemente, me permito recomendar la aprobación del trabajo y que sea aceptado para la discusión en el Examen Privado de Tesis.

Sin otro particular, aprovecho la ocasión para exteriorizarle altas muestras de consideración y estima.

Atentamente,

Lic. Juan Carlos Díaz
Colegiado CPA No. 8799



FACULTAD DE
CIENCIAS ECONOMICAS

Edificio "S-8"
Ciudad Universitaria, Zona 12
Guatemala, Centroamérica

**DECANATO DE LA FACULTAD DE CIENCIAS ECONOMICAS. GUATEMALA,
VEINTICINCO DE MAYO DE DOS MIL QUINCE.**

Con base en el Punto cuarto, inciso 5.1, subinciso 5.1.1 del Acta 14-2015 de la sesión celebrada por la Junta Directiva de la Facultad el 12 de mayo de 2015, se conoció el Acta AUDITORÍA 39-2015 de aprobación del Examen Privado de Tesis, de fecha 16 de marzo de 2015 y el trabajo de Tesis denominado: "EL PAPEL DEL CONTADOR PÚBLICO Y AUDITOR COM AUDITOR INTERNO EN LA ELABORACIÓN DE PROCEDIMIENTOS DE CONTROL INTERNO EN LA PREVENCIÓN DE FRAUDES INFORMÁTICOS EN EL ÁREA DE CUENTAS POR COBRAR PARA UNA EMPRESA DE TRANSPORTE TERRESTRE", que para su graduación profesional presentó el estudiante **ADRIÁN PINEDA GARCÍA**, autorizándose su impresión.

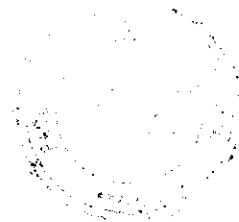
Atentamente,

"ID Y ENSEÑAR A TODOS"


LIC. CARLOS ROBERTO CABRERA MORALES
SECRETARIO

LIC. LUIS ANTONIO SUÁREZ ROLDÁN
DECANO INTERINO

Smp.



Ingrid
ABUSANO

DEDICATORIA

- A DIOS: Por brindarme el conocimiento, la fortaleza y la Iluminación en los momentos en que más los necesitaba para concluir mi carrera.
- A MIS PADRES: Adrián Pineda (espero que en el cielo se sienta orgulloso por este logro) Juana García de Pineda (Gracias por todos sus consejos por acompañarme en mis noches de desvelo y por todas las oraciones, yo sé que sin ellas me hubiera sido difícil concluir una de mis metas).
- A MIS HIJOS: Anaby Pineda y Adrián Pineda, espero que mi triunfo les sirva de inspiración, son mi fortaleza los quiero mucho.
- A MIS HERMANOS: Gracias por apoyarme siempre son mi sangre y son muy importantes en mi vida. (Y los que ya no están conmigo con mucho cariño sé que desde el cielo tengo sus bendiciones y nunca los olvidares)
- A MI FAMILIA: Gracias por todo el apoyo.
- A MIS AMIGOS: Se les agradece sus consejos, especialmente a mi asesor de Tesis Lic. Juan Carlos Díaz.
- A: Mi supervisor de Tesis Lic. Giovanni Garrido. (Muchas gracias por todo)
- A: Esas personas importantes en mi vida, que siempre estuvieron listas para brindarme toda su ayuda, ahora me toca regresar un poquito de todo lo inmenso que me han otorgado.

ÍNDICE

INTRODUCCIÓN	i
---------------------	----------

CAPÍTULO I

EMPRESA DE TRANSPORTE TERRESTRE Y LA AUDITORÍA INTERNA

1.1 EMPRESA DE TRANSPORTE TERRESTRE

1.1.1 Definición de empresa	1
1.1.2 Clasificación de empresas	1
1.1.3 Empresas de transporte terrestre	4
1.1.4 Antecedentes de la empresa de transporte terrestre objeto de estudio	5

1.2 AUDITORÍA INTERNA

1.2.1 Definición	11
1.2.2 Objetivo	12
1.2.3 Alcance	12
1.2.4 Riesgos de auditoría	13
1.2.5 Funcionamiento	18
1.2.6 Normas internacionales para el ejercicio profesional de Auditoría interna (NIEPAI)	19
1.2.7 La auditoría interna y el control interno en informática	20
1.2.8 El contador público y auditor como auditor interno	25

CAPÍTULO II

ÁREA DE CUENTAS POR COBRAR

2.1 CUENTAS POR COBRAR

2.1.1 Definición	29
2.1.2 Clasificación	29

2.1.3 Naturaleza	30
2.1.4 Registro contable	30
2.1.5 Presentación en los estados financieros	33
2.1.6 Cuentas incobrables	33
2.1.7 Normas internacionales de contabilidad (NIC).	35
2.1.8 Marco conceptual	36

CAPÍTULO III

SISTEMAS INFORMÁTICOS Y PROCEDIMIENTOS DE CONTROL INTERNO EN LA PREVENCIÓN DE FRAUDES EN EL ÁREA DE CUENTAS POR COBRAR

3.1 SISTEMAS DE INFORMACIÓN COMPUTARIZADA

3.1.1 Definición	38
3.1.2 Aplicación	38
3.1.3 Seguridad	39
3.1.4 Humanware	40
3.1.5 Software	40
3.1.6 Hardware	42

3.2 FRAUDE INFORMÁTICO

3.2.1 Fraude	43
3.2.2 Definición	44
3.2.3 Origen	44
3.2.4 Daños o modificaciones de programas o datos computarizados	45
3.2.5 Clasificación	46
3.2.6 Factores que facilitan el fraude	49
3.2.7 Clasificación del fraude en auditoría	49
3.2.8 Tipos de fraude	50
3.2.9 Técnicas para realizar fraudes electrónicos	50

3.2.10 Fraudes en el área de cuentas por cobrar	51
3.2.11 Prevención del fraude en las cuentas por cobrar	51

3.3 PROCEDIMIENTOS DE CONTROL INTERNO PARA LA PREVENCIÓN DE FRAUDES INFORMÁTICOS EN EL ÁREA DE CUENTAS POR COBRAR

3.3.1 Definición	55
3.3.2 Procedimientos de control interno para la organización del área de contabilidad	55
3.3.3 Procedimientos de control interno en el área de cuentas por cobrar	60
3.3.4 Procedimientos de control interno de: entrada de datos, el procesamiento de información y la emisión de resultados	61
3.3.5 Procedimientos de control interno para la seguridad del área de sistemas	66

CAPÍTULO IV

EL PAPEL DEL CONTADOR PÚBLICO Y AUDITOR, COMO AUDITOR INTERNO EN LA ELABORACIÓN DE PROCEDIMIENTOS DE CONTROL INTERNO EN LA PREVENCIÓN DE FRAUDES INFORMÁTICOS EN EL ÁREA DE CUENTAS POR COBRAR PARA UNA EMPRESA DE TRANSPORTE TERRESTRE (CASO PRÁCTICO)

4.1 ANTECEDENTES DE LA EMPRESA	69
4.2 CONSTITUCIÓN Y ORGANIZACIÓN	71
4.3 ORGANIGRAMA	76
4.4 GENERALIDADES	77
4.5 TRABAJO A DESARROLLAR	79
4.6 PAPELES DE TRABAJO	81
4.7 INFORME DE AUDITORÍA	93
PROCEDIMIENTOS DE AUDITORÍA	100
CONCLUSIONES	119

RECOMENDACIONES	120
REFERENCIAS BIBLIOGRÁFICAS	121
ANEXO	
GLOSARIO	

ÍNDICE
Tablas y Figuras

Formato No.	No. de página
1. Figura 1	15
2. Tabla 1	71
3. Figura 2	76

CAPÍTULO I

EMPRESA DE TRANSPORTE TERRESTRE Y LA AUDITORÍA INTERNA

1.1 EMPRESA DE TRANSPORTE TERRESTRE

Es la encargada de trasladar cosas, bienes o mercancías de un lugar a otro por vía terrestre. La prestación de dicho servicio de carácter lucrativa ya que la misma cubre riesgos en el traslado de mercaderías, cosas o bienes.

1.1.1 Definición de empresa

“Es una organización, institución o industria, dedicada a actividades o persecución de fines económicos o comerciales, para satisfacer las necesidades de bienes y/o servicios de los demandantes, a la par de asegurar la continuidad de la estructura productivo-comercial así como sus necesarias inversiones”.(16:1)

El artículo 655 del Código de Comercio de Guatemala, indica que “se entiende por empresa mercantil el conjunto de trabajo, de elementos materiales y de valores incorpóreos coordinados, para ofrecer al público, con propósito de lucro y de manera sistemática, bienes o servicios”. (6:103)

1.1.2 Clasificación de empresas

El avance tecnológico y económico ha originado la existencia de una gran diversidad de empresas. Aplicar la administración más adecuada a la realidad y a las necesidades específicas de cada una determinará el éxito de la función empresarial. Resulta pues importante definir las diferentes clases de empresas existentes en el medio guatemalteco.

✓ **Por sectores económicos**

- a) **Industriales:** la actividad primordial de este tipo de empresas es la producción de bienes mediante la transformación de la materia o extracción de materias primas.

Las industrias a su vez se clasifican en:

- ✓ **Extractivas:** cuando se dedican a la extracción de recursos naturales, ya sea renovable y no renovable.
- ✓ **Manufactureras:** son empresas que transforman la materia prima en productos terminados.

b) **Comerciales:** son intermediarias entre productor y consumidor; su función primordial es la compra y venta de productos terminados.

Pueden clasificarse en:

- ✓ **Mayorista:** venden a gran escala o a grandes rasgos.
- ✓ **Minorita (detallista):** venden al por menor.
- ✓ **Comisionista:** venden de lo que no es suyo, dan consignación.

c) **Agropecuarias:** son aquellas que explotan a grandes cantidades los productos agrícolas, pecuarios, del campo y sus recursos.

d) **Servicio:** son aquellas que brindan servicio a la comunidad que a su vez se clasifican en:

- ✓ **Transporte**
- ✓ **Turismo**
- ✓ **Instituciones financieras**
- ✓ **Servicios públicos**
- ✓ **Servicios privados**
- ✓ **Educación**
- ✓ **Finanzas**
- ✓ **Salud**

✓ **Por el origen de capital**

a) **Público:** su capital proviene del estado o gobierno.

b) **Privado:** son aquellas en que el capital proviene de particulares.

c) **Economía mixta:** el capital proviene una parte del estado y la otra de particulares.

✓ **Por su tamaño**

No hay unanimidad en los economistas a la hora de establecer qué es una empresa grande o pequeña, puesto que no existe un criterio único para medir el tamaño de la empresa. Los principales indicadores son: el volumen de ventas, el capital propio, número de trabajadores, beneficios, otros, el más utilizado suele ser según el número de trabajadores. Este criterio delimita la magnitud de las empresas de la forma mostrada a continuación:

- a) **Microempresa:** si posee de 10 o menos trabajadores.
- b) **Pequeña empresa:** si tiene un número entre 11 y 49 trabajadores.
- c) **Mediana empresa:** si tiene un número entre 50 y 250 trabajadores.
- d) **Gran empresa:** si posee más de 250 trabajadores.
- e) **Multinacional:** es aquella empresa que cuenta con operaciones en varios países.

✓ **Por su ámbito geográfico**

En función del ámbito geográfico en el que las empresas realizan su actividad, se pueden clasificar en:

- a) **Empresas locales:** son aquellas empresas que venden sus productos o servicios dentro de una localidad determinada.
- b) **Empresas nacionales:** son aquellas empresas que actúan dentro de un solo país.
- c) **Empresas multinacionales o internacionales:** son aquellas que actúan en varios países.
- d) **Empresas transnacionales:** las empresas transnacionales son las que no solo están establecidas en su país de origen, sino que también se constituyen en otros países, para realizar sus actividades mercantiles no solo de venta y compra, sino de producción en los países donde se han establecido.

✓ **Por el número de propietarios**

a) **Empresas individuales:** si sólo pertenece a una persona. Ésta puede responder frente a terceros con todos sus bienes, es decir, con responsabilidad ilimitada, o sólo hasta el monto del aporte para su constitución, en el caso de las empresas individuales de responsabilidad limitada. Es la forma más sencilla de establecer un negocio y suelen ser empresas pequeñas o de carácter familiar.

b) **Empresas de sociedades:** constituidas por varias personas. Dentro de esta clasificación están: la sociedad anónima, la sociedad colectiva, la sociedad comanditaria, la sociedad de responsabilidad limitada.

✓ **Por la función social**

a) **Lucrativas:** se constituye la empresa con el propósito de explotar y ganar más dinero.

b) **No lucrativas:** son empresas que su factor social es la ayuda y apoyo de la comunidad.

1.1.3 Empresa de transporte terrestre

Es la encargada de trasladar cosas, bienes o mercancías de un lugar a otro por vía terrestre. La prestación de dicho servicio es de carácter lucrativo ya que la misma cubre riesgos en el traslado de mercaderías, cosas o bienes.

✓ **Empresa de transporte autorizada**

Empresas de transporte legalmente constituidas que cuentan con autorizaciones para realizar actividades propias del régimen de tránsito aduanero.

✓ **Transporte internacional de mercancías**

Consiste en el traslado de bienes de un país a otro mediante los sistemas de tránsito aduanero internacional.

✓ **Autoridades aduaneras**

Son las responsables de efectuar el control aduanero como lo dictan los acuerdos y convenios internacionales, sin olvidar la legislación nacional de dichos países, por ejemplo en el caso de aduanas de partida, deben verificar que en la documentación presentada hayan sido declarados correctamente los medios de transporte, unidades de carga y mercancías que se transportan, debiendo colocar los precintos aduaneros, para asegurar y autorizar el inicio del tránsito aduanero por la ruta y plazo establecido.

✓ **Contrato de transporte**

Se suscribe entre el transportista y el cliente, donde se describen las condiciones del tránsito, el lugar de recepción y entrega, plazos y condiciones de las mercancías.

1.1.4 Antecedentes de la empresa de transporte terrestre objeto de estudio

Es una empresa unidad de análisis Roxaluna, S. A., fue fundada en el año 2001 en la ciudad de Guatemala, en constante evolución, se dedica a prestar servicio de transporte terrestre nacional desde su fundación se ha caracterizado por contar con tecnología moderna para el registro de sus operaciones y procesos administrativos.

Esta empresa ofrece una amplia gama de servicios como transporte de bienes y cosas, maquinaria pesada y liviana. Cuenta con transporte idóneo para prestar un servicio de calidad y de satisfacción para el cliente.

✓ **Transporte terrestre nacional**

- a) Transporte de cargas interdepartamentales (Escuintla, Izabal, San Marcos, Chiquimula, otros.)
- b) Transporte de carga en camiones puerta a puerta en toda Guatemala.

c) Transporte terrestre internacional.

✓ **Equipo que tienen para prestar los diferentes servicios son:**

- a) Equipo especializados en transporte de mobiliario y menaje de casa.
- b) Equipo para cargas refrigeradas.
- c) Equipo para cargas sobredimensionadas.
- d) Equipo para cargas consideradas peligrosas.

✓ **Estructura según su constitución jurídica**

Las empresas pueden clasificarse también según su constitución jurídica, en este caso se constituyó por medio de una Sociedad Anónima la cual según el Código de Comercio de Guatemala en su artículo No. 86 se define como: “es la que tiene el capital dividido y representado en acciones la responsabilidad de los accionistas está limitada al pago de las acciones que hubiera suscrito.” (6:14).

En el artículo No. 87 el cual define la denominación de la sociedad de la siguiente manera: “La Sociedad Anónima se identifica con una denominación, la cual se podrá formar con el grado obligatorio de la leyenda: Sociedad Anónima que podrá abreviarse como S. A.” (6:14).

✓ **Legislación aplicable**

Como toda empresa constituida en territorio guatemalteco debe observar el cumplimiento de la legislación para tener sus operaciones y registros como estas lo regulen, por lo que a continuación se mencionan algunas de las que debe observar:

Formalizar una empresa, implica cumplir con los trámites de inscripción, registros y operaciones que la ley establece según el tipo de empresas y el giro de la misma, es decir la actividad a la que se dedica. Los aspectos más importantes de una empresa formal son:

- a) Contar con la Patente de Comercio
- b) Cumplir con el pago de impuestos
- c) Cumplir con las regulaciones de operación que tienen que ver con aspectos laborales, sanitarios y de protección al medio ambiente.

Las leyes otorgan derechos y obligaciones, desde el momento de constitución de las empresas, según el Código de Comercio de la República de Guatemala.

a) Registro mercantil

Institución del Gobierno cuya misión es registrar, certificar, dar seguridad jurídica a todos los actos relacionados con las actividades mercantiles que realicen las personas.

Deberá registrar el tipo de empresa que se desea inscribir, (comerciante o empresa individual o algún tipo de sociedad mercantil). La empresa una vez registrada recibirá su Patente de Comercio, que es el documento que acredita la inscripción de la empresa ante el Registro Mercantil.

b) Superintendencia de administración tributaria, SAT

Entidad estatal descentralizada, que ejerce con exclusividad las funciones de administración tributaria contenidas en la legislación. Su misión es recaudar los recursos (impuestos) provenientes de los actos gravados. Toda empresa debe registrar sus operaciones ante la Superintendencia de Administración Tributaria (SAT), quién autorizará los libros contables, facturas a utilizar, cajas o máquinas registradoras.

Las empresas estarán afectas a los distintos impuestos, según su actividad, entre ellos mencionaremos algunos:

a) Impuesto al valor agregado (IVA)

Esta ley, contenida en el Decreto 27-92, establece un Impuesto al Valor Agregado sobre los actos y contratos gravados por ésta, cuya administración, control, recaudación y fiscalización corresponde a la

Superintendencia de Administración Tributaria (SAT). Dichos actos y contratos afectan, las encontramos de forma específica en el hecho generador del artículo tres (3) de la misma.

Las empresas afectas a las disposiciones de esta ley, pagarán el impuesto de una tarifa única del doce por ciento (12%) sobre la base imponible, porcentaje que deberá estar incluida en el precio de venta de los bienes o el valor de los servicios.

La suma neta que el contribuyente debe enterar al fisco mensualmente, es la diferencia entre el total de débitos y el total de créditos fiscales generados (Art. 19 ley).

b) Impuesto sobre la renta (ISR)

Toda empresa esta afecta a las disposiciones legales contenidas en el Decreto 10-2012 LEY DE ACTUALIZACIÓN TRIBUTARIA LIBRO I. Quedan afectas al impuesto todas las rentas y ganancias de capital obtenidas en el territorio nacional. El impuesto se genera cada vez que se producen rentas gravadas y se determina de conformidad con lo que establece dicha ley. Son contribuyentes del impuesto, las personas individuales y jurídicas, domiciliadas o no en el país, que obtengan rentas en el país independientemente de su nacionalidad o residencia y por lo tanto están obligadas al pago del impuesto cuando se verifique el hecho generador del mismo.

En este régimen, el impuesto se determinará y pagará por trimestres vencidos, sin perjuicio de la liquidación definitiva del período anual.

c) Impuesto de solidaridad, ISO

Las disposiciones legales de esta ley, Decreto número 73-2008, establece un hecho generador por la realización de actividades

mercantiles o agropecuarias en el territorio nacional, para las personas, entes o patrimonios a que se refiere el 12 artículo uno de la ley y que los ingresos brutos sean superiores al 4%. Dicha ley establece algunas exenciones para algunas entidades tal como se establece en el artículo cuatro (4) de la misma.

El tipo impositivo que establece, es la del 1%, que será multiplicado por la base imponible establecida por las dos opciones que establece el artículo 7, que no es más que; la cuarta parte de monto del activo neto o la cuarta parte de los ingresos brutos.

d) Impuesto de timbres fiscales y del papel sellado especial para protocolos

Esta ley, está contenida en el Decreto 37-92 y recae sobre los documentos que contienen actos y contratos que se expresan en la ley según el artículo dos (2) de la misma, ya que los sujetos pasivos son; quienes emitan, suscriban u otorguen documentos que contengan actos o contratos objeto de tal emisión, suscripción u otorgamiento. La tarifa del impuesto es del 3% aplicado al valor de los actos y contratos afectos, la cual no podrá ser inferior al que conste en los registros públicos, matrículas, catastro o en los listados oficiales.

e) Código tributario

Las normas del Código Tributario Decreto 6-91, son aplicables a las infracciones y sanciones, estrictamente en materia tributaria, salvo lo que dispongan las normas especiales que establezcan las leyes que regulan cada tributo (Art. 67), Es así, como las empresa deberán tener sumo cuidado en no cometer ningún tipo de acción u omisión que implique violación de normas tributarias de índole sustancial o formal, ya que será sancionada por la Administración Tributaria (SAT), en tanto no

constituya delito o falta sancionados conforme a la legislación penal.(Art. 69)

f) Ley de productos financieros (IPF)

Según esta Ley Decreto 26-95 del Congreso de la República, es que grava los ingresos por intereses de cualquier naturaleza generados en el momento del pago o acreditamiento de intereses. Están obligadas las personas individuales o jurídicas domiciliadas en el país, que obtengan ingresos por concepto de intereses con excepción de las personas sujetas a la fiscalización de la Superintendencia de Bancos (SB). La base imponible de este impuesto lo constituye la totalidad de los ingresos por concepto de intereses multiplicado por el tipo impositivo del 10%,

g) Código de trabajo

Según Decreto 1441, este código establece los derechos y obligaciones de patronos y trabajadores, con ocasión del trabajo y crea instituciones para resolver sus conflictos, tal como lo señala el artículo uno (1) de la ley. Dicha ley son adoptadas por todas las empresas en Guatemala, ya que norma la relación patrono-trabajador, mediante un contrato individual de trabajo.

También deberá regirse por otras leyes, como:

- a) Código Penal (Decreto 17-73 y sus reformas).
- b) Disposiciones Legales para el Fortalecimiento de la Administración (Decreto 20-2006).
- c) Ley Orgánica del Instituto Guatemalteco de Seguridad Social (Decreto 295).
- d) Código Aduanero Uniforme Centroamericano (resolución No. 223-2008)

El cumplimiento de las leyes citadas, inician desde que se formalice la empresa, mediante la escritura de constitución y el nombramiento del representante legal.

La empresa debe estar registrada como patrono ante el Instituto Guatemalteco de Seguridad Social (IGSS), para efectuar las retenciones y pago de la cuota laboral, así como de las cuotas patronales.

1.2 AUDITORÍA INTERNA

1.2.1 Definición

“Es un control de dirección que tiene por objeto la medida y evaluación de la eficacia de otros controles. La auditoría interna surge con posterioridad a la auditoría externa por la necesidad de mantener un control permanente y más eficaz dentro de la empresa y de hacer más rápida y eficaz la función del auditor externo.

Generalmente la auditoría interna clásica se ha venido ocupando fundamentalmente del sistema de control interno, es decir, del conjunto de medidas, políticas y procedimientos establecidos en las empresas para proteger el activo, minimizar las posibilidades de fraude, incrementar la eficiencia operativa y optimizar la calidad de la información económico-financiera. Se ha centrado en el terreno administrativo, contable y financiero.

La necesidad de la auditoría interna se pone de manifiesto en una empresa a medida que ésta aumenta en volumen, extensión geográfica y complejidad, lo que hace imposible el control directo de las operaciones por parte de la dirección.

Con anterioridad, el control lo ejercía directamente la dirección de la empresa por medio de un permanente contacto con sus mandos intermedios y hasta con los empleados de la empresa. En la gran empresa moderna ésta peculiar forma de ejercer el control ya no es posible hoy día y de ahí la emergencia de la llamada auditoría interna”. (25:2)

1.2.2 Objetivo

El objetivo principal es ayudar a la dirección en el cumplimiento de sus funciones y responsabilidades proporcionándole análisis objetivos, evaluaciones, recomendaciones y todo tipo de comentarios pertinentes sobre las operaciones examinadas. Este objetivo se cumple a través de otros más específicos como los siguientes: (25:2).

- a) "Apoyar a la máxima autoridad, ofreciendo servicios de aseguramiento y consultoría en las operaciones administrativas, financieras y operativas, que cumplan con las políticas, procedimientos y reglamentaciones legales en la toma de decisiones.
- b) Velar por las buenas prácticas en la administración de la Institución y fiscalizar en apego a la normativa que regula la gestión administrativa.
- c) Evaluar el grado de cumplimiento de las operaciones frente a los planes establecidos.
- d) Evaluar permanentemente que se cumplan los controles internos en el área financiera y operacional.
- e) Recomendar medidas ya sean preventivas o correctivas para fortalecer el control interno.
- f) Evaluar el sentido de responsabilidad y el uso eficaz o correcto en lo financiero. (25:2)

1.2.3 Alcance

Todos los profesionales vinculados al ejercicio de la Auditoría y los empresarios conocen de la vital importancia que tiene para el éxito del negocio contar con un equipo de Auditoría Interna que responda a los intereses del mismo, se constituya un factor aliado de la alta jefatura de la entidad, garantizará la correcta administración, uso y control de los recursos humanos, materiales y financieros. (25:2)

Por lo que en su alcance se puede mencionar:

- a) Verificar eventos pasados.

- b) Prevenir eventos futuros.
- c) Examinar la actividad económica.
- d) Comprobar eventos financieros.
- e) Reportar e informar a la más alta dirección.
- f) Debe ser totalmente independiente respecto a las partes auditadas.
- g) Desarrollar su actividad en casi la totalidad de las áreas de la organización.

El alcance de la auditoría interna debe incluir la revisión y la evaluación de la estructura del control interno, para determinar si el mismo es efectivo y eficiente. El propósito de la revisión es la estructura del control interno, determinar si se cumplen los objetivos elementales del mismo. El alcance del trabajo de auditoría interna abarca la ejecución del plan de trabajo: sin embargo, la gerencia y la junta de accionistas proporcionan una dirección sobre el mismo.

1.2.4 Riesgos de auditoría

Un riesgo de auditoría es aquel que existe en todo momento por lo cual genera la posibilidad de que un auditor emita una información errada por el hecho de no haber detectado errores o faltas significativas que podría modificar por completo la opinión dada en un informe.

La posibilidad de existencia de errores puede presentarse en distintos niveles, por lo tanto se debe analizar de la forma más apropiada para observar la implicación de cada nivel sobre las auditorías que vayan a ser realizadas.

Es así como se han determinado tres tipos de riesgos los cuales son: riesgo inherente, riesgo de control y riesgo de detección.

✓ Riesgo en la auditoría

“El riesgo en auditoría puede ser considerado como una combinación entre la posibilidad de la existencia de errores significativos o irregularidades en

los estados financieros (a lo que llamamos riesgo relativo) y el hecho de que los mismos no sean descubiertos por medio de los procedimientos de control interno del cliente o del trabajo de auditoría (riesgo probable)".
(14:75)

Durante la etapa de planeación técnica se identifican los riesgos significativos y aplicando la capacidad y el criterio para seleccionar los procedimientos de auditoría se puede reducir el riesgo a un nivel aceptable.

- ✓ **Clases de riesgos que tiene el auditor en la ejecución de una auditoría**
El auditor puede estar sujeto a varios riesgos en la ejecución de su trabajo, siendo los principales:

- ✓ **Riesgo profesional por asociación con el cliente**

Es el riesgo de sufrir un perjuicio en la reputación profesional o en el patrimonio del auditor por asociación con un cliente. Lo que se debe evaluar para mitigar este riesgo es:

- Relaciones con posibles clientes.
- Factores que afectan el riesgo profesional.
- Documentación de la evaluación del riesgo profesional.
- Reevaluación de la vinculación con clientes existentes.

Los factores que pueden afectar el riesgo profesional son:

- **Negocio**, se refiere a la viabilidad de los productos o servicios ofrecidos, perspectivas de la empresa y de la industria y riesgos inherentes del negocio.
- **Posición pública**, que incluye la visibilidad pública, compromiso público de obtener ganancias proyectadas, litigios significativos, investigaciones legales y antecedentes de problemas de cumplimiento legal.

- Estructura corporativa, que se refiere a la complejidad de la estructura de las empresas del grupo.
- Empresas vinculadas, se refiere al alcance de las transacciones con empresas vinculadas.

✓ **Riesgos de emitir un informe de auditoría inadecuado**

El riesgo de auditoría está integrado por el efecto combinado de los tres tipos diferentes de riesgo que se mencionan a continuación:

Figura 1
Cualitativo cuantitativo del riesgo

Alto	mas de 60%
Medio	de 40 a 60%
Bajo	menos de 40%

Nota:

El riesgo es cualitativo y cuantitativo y muestra las posibilidades alto, medio y bajo de que el auditor emita un informe erróneo.

Relación de las Normas Internacionales de Auditoría (NÍAS) 315 y 330 con el entendimiento del riesgo empresarial

Las Normas Internacionales de Auditoría, son lineamientos generalmente aceptados en todo el mundo, cuyo objetivo son ser el marco de referencia sobre el cual el auditor debe ejecutar su trabajo.

Las NÍAS 315 y 330 se relacionan directamente con la evaluación del riesgo empresarial y con los procedimientos que el auditor debe aplicar en respuesta a éstos; desde las dos perspectivas existentes: como CPA y como consultor. A continuación describimos brevemente el contenido de las normas indicadas.

Entendimiento de la entidad y su entorno y evolución de los riesgos de representación errónea de importancia relativa (NÍA 315)

El objetivo de esta norma es proporcionar guías para obtener un entendimiento del negocio y su entorno, incluyendo su control interno, y para evaluar los riesgos de representación errónea de importancia relativa en una auditoría de estados financieros, ya sea por fraude o error; esta evaluación le servirá al auditor para diseñar y desempeñar procedimientos adicionales en la ejecución de su trabajo.

Los requisitos esenciales que debe observar el auditor de acuerdo a esta norma son:

- Procedimientos de evaluación del riesgo y fuentes de información sobre la entidad y su entorno, incluyendo su control interno.
- Entendimiento de la entidad y su entorno, incluyendo su control interno; con el objetivo de identificar y evaluar los riesgos de representación errónea.
- Evaluación de los riesgos de representación errónea. En esta etapa, el auditor debe identificar los riesgos y relacionarlos con lo que pueda estar mal al nivel de representación de información, considerar la importancia y probabilidad de los riesgos.
- Comunicación con los encargados de la administración.
- Documentación, que se refiere a la forma en que el auditor debe documentar los riesgos identificados y evaluados.

Procedimientos del auditor en respuesta a los riesgos evaluados (NÍA 330)

El objetivo de esta norma es proporcionar guías para determinar respuestas globales y diseñar y desempeñar procedimientos adicionales de auditoría para responder a los riesgos evaluados con los procedimientos indicados en la NÍA 315. Los requerimientos de esta norma se resumen en:

- Implementar respuestas globales para atender los riesgos.

- Aplicar procedimientos de auditoría que responda a los riesgos de representación errónea.
- Evaluación de los suficiente y apropiado de la evidencia de auditoría obtenida y la forma en que debe documentarse.

Definición de riesgo

"El riesgo se define como "contingencia o proximidad de un daño". (14:1)

El término riesgo, se enfoca a la eventualidad o posibilidad de que un evento esperado pueda o no ocurrir.

El riesgo puede ser considerado como una combinación entre la posibilidad de la existencia de eventos que tengan efectos negativos o de consecuencias perjudiciales para la entidad y oportunidades de negocio o crecimiento aún no descubiertas.

Tipos de riesgos de auditoría

- a) **Riesgo inherente:** este tipo de riesgo tiene que ver exclusivamente con la actividad económica o negocio de la empresa, independientemente de los sistemas de control interno que allí se estén aplicando. Entre los factores que llevan a la existencia de este tipo de riesgos está la naturaleza de las actividades económicas, como también la naturaleza de volumen tanto de transacciones como de productos y/o servicios, además tiene relevancia la parte gerencial y la calidad de recurso humano con que cuenta la entidad.

- b) **Riesgo de control:** aquí influye de manera muy importante los sistemas de control interno que estén implementados en la empresa y que en circunstancias lleguen a ser insuficientes o inadecuados para la aplicación y detección oportuna de irregularidades. Es por esto la necesidad y relevancia que una administración tenga en

- Aplicar procedimientos de auditoría que responda a los riesgos de representación errónea.
- Evaluación de los suficiente y apropiado de la evidencia de auditoría obtenida y la forma en que debe documentarse.

Definición de riesgo

“El riesgo se define como “contingencia o proximidad de un daño”. (14:1)

El término riesgo, se enfoca a la eventualidad o posibilidad de que un evento esperado pueda o no ocurrir.

El riesgo puede ser considerado como una combinación entre la posibilidad de la existencia de eventos que tengan efectos negativos o de consecuencias perjudiciales para la entidad y oportunidades de negocio o crecimiento aún no descubiertas.

Tipos de riesgos de auditoría

- a) **Riesgo inherente:** este tipo de riesgo tiene que ver exclusivamente con la actividad económica o negocio de la empresa, independientemente de los sistemas de control interno que allí se estén aplicando. Entre los factores que llevan a la existencia de este tipo de riesgos está la naturaleza de las actividades económicas, como también la naturaleza de volumen tanto de transacciones como de productos y/o servicios, además tiene relevancia la parte gerencial y la calidad de recurso humano con que cuenta la entidad.

- b) **Riesgo de control:** aquí influye de manera muy importante los sistemas de control interno que estén implementados en la empresa y que en circunstancias lleguen a ser insuficientes o inadecuados para la aplicación y detección oportuna de irregularidades. Es por esto la necesidad y relevancia que una administración tenga en

constante revisión, verificación y ajustes los procesos de control interno.

Entre los factores relevantes que determina este tipo de riesgo son los sistemas de información, contabilidad y control.

- c) **Riesgo de detección:** este tipo de riesgo está directamente relacionado con los procedimientos de auditoría por lo que se trata de la no detección de la existencia de errores en el proceso realizado.

La responsabilidad de llevar a cabo una auditoría con procedimientos adecuados es total responsabilidad del grupo auditor, es tan importante este riesgo que bien trabajado contribuye a debilitar el riesgo de control y el riesgo inherente de la compañía.

1.2.5 Funcionamiento

- a) Implementar las políticas dictadas por la junta de accionistas en materia de auditoría.
- b) Monitorear la correcta secuencia de los ciclos de transacciones; los sistemas de operación aplicables.
- c) Revisar y aprobar el programa anual de trabajo de auditoría interna.
- d) Recibir y comentar los informes de auditoría externa.
- e) Opinar sobre la contratación de los servicios de auditoría externa.
- f) Recibir y aprobar los dictámenes del auditor externo.
- g) Dar seguimiento a las cartas de recomendaciones al control interno.
- h) Vigilar por las buenas relaciones entre auditoría interna y externa.
- i) Preparar informes para la junta de accionistas sobre resultados relevantes de auditoría interna y,
- j) Servir de enlace entre la auditoría externa con la junta de accionistas cuando se requiere.

1.2.6 Normas internacionales para el ejercicio profesional de auditoría interna (NIEPAI)

"Son procedimientos profesionales promulgados por el consejo de normas de auditoría interna del Instituto de Auditores Internos, que describen los requerimientos para desempeñar un amplio rango de actividades de auditoría interna y para evaluar el desempeño de la auditoría interna". (28:22)

Las normas son requisitos enfocados a principios, de cumplimiento obligatorio, que consisten en:

- a) Declaraciones de requisitos básicos para el ejercicio de la auditoría interna y para evaluar la eficacia de su desempeño, de aplicación internacional a nivel de las personas y a nivel de las organizaciones.
- b) Interpretaciones que aclaran términos o conceptos dentro de las declaraciones.

La estructura de las normas está formada por:

- a) **sobre atributos**: que tratan las características de las organizaciones y las personas que prestan servicios de auditoría interna.
- b) **Las normas sobre desempeño**: que describen la naturaleza de los servicios de auditoría interna y proporcionan criterio de calidad con los cuales puede evaluarse el desempeño de estos servicios. Las normas sobre atributos y sobre desempeño se aplican a todos los servicios de auditoría interna.
- c) **Las normas de implantación**: amplían las normas sobre atributos y desempeño proporcionando los requisitos aplicables a las actividades de aseguramiento y consultoría.

Los propósitos de las normas son:

- a) Definir principios básicos que representen el ejercicio de la auditoría interna tal como este debiera ser.
- b) Proporcionar un marco para ejercer y promover un amplio rango de actividades de auditoría interna de valor añadido.

- c) Establecer las bases para evaluar el desempeño de la auditoría interna.
- d) Fomentar la mejora de los procesos y operaciones de la organización.

1.2.7 La auditoría interna y el control interno en informática

✓ Control interno

“El control interno es una función que tiene por objeto salvaguardar y preservar los bienes de la empresa, evitar desembolsos indebidos de fondos y ofrecer la seguridad de que no se contraerán obligaciones sin autorización.

Una segunda definición definiría al control interno como: el sistema conformado por un conjunto de procedimientos (reglamentaciones y actividades) que interrelacionadas entre sí, tienen por objetivo proteger los activos de la organización”. (25:04)

✓ Importancia del control interno

“Permite el manejo adecuado de los bienes, funciones e información de una empresa determinada, con el fin de generar una indicación confiable de su situación y sus operaciones en el mercado”. (25:04)

✓ Objetivos del control interno

Se reconocen cuatro objetivos primordiales:

- Protección de los activos de la entidad.
- Obtención de información financiera confiable y oportuna.
- Promoción de la eficiencia operacional.
- Adhesión a las políticas de la empresa.

✓ Clasificación del control interno

El control interno se divide en dos elementos:

✓ **Control interno contable**

“Consiste en el plan de organización y los procedimientos y registros referentes a la salvaguarda de los activos y a la fiabilidad de los registros financieros”. (25:06)

En consecuencia está diseñado para proporcionar seguridad razonable de que:

- Las transacciones se efectúan de acuerdo con la autorización de la dirección.
- Las transacciones se registran para permitir la preparación de estados financieros y mantener el control sobre los activos.
- El acceso a los activos está permitido únicamente con la autorización de la dirección.
- El activo contabilizado se compara con el existente a intervalos de tiempos razonables y se adoptan las medidas correspondientes en el caso de que se detecten diferencias.

✓ **Control interno administrativo**

“Incluye el plan de organización y los procedimientos y registros relacionados con los procesos de decisión que llevan a la autorización por parte de la dirección, de acuerdo con esto se enfoca a la promoción de la eficiencia operativa y que la ejecución de las operaciones se adhieran a las políticas prescritas por la administración”. (25:06)

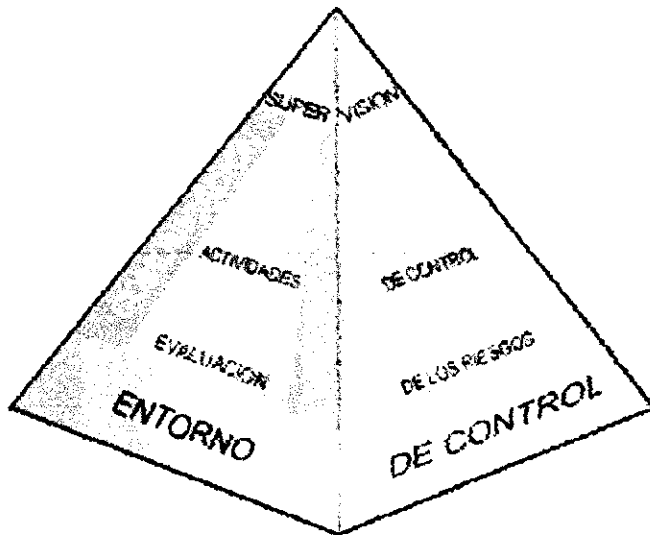
✓ **Aspectos a considerar en relación al control interno**

- Organización, que incluye la dirección, coordinación, asignación y segregación de funciones.
- Procedimientos, que se refiere a la planeación y sistematización, los registros y formas así como los informes a presentar.
- Personal, que incluye el entrenamiento, moralidad, eficiencia y retribución al recurso humano.

- Supervisión, si existe una adecuada planeación y sistematización, es necesario ejercer una adecuada supervisión en forma sistemática en cada uno de los aspectos referidos anteriormente.

✓ **Elementos del control interno**

Los elementos del control interno se definen a continuación.



a) Ambiente de control

“Representa el ambiente colectivo de varios factores en establecer, realzar o mitigar la efectividad de políticas específicas.

El análisis del ambiente de control, refleja la actitud, conciencia y acciones en general del Consejo de administración, la Gerencia, los dueños y otros funcionarios, en relación a la importancia de control y su incidencia en la entidad”. (14:73)

b) Evaluación de los riesgos

Las organizaciones, cualquiera sea su tamaño, se enfrentan a diversos riesgos de origen externos e internos que tienen que ser evaluados. Una condición previa a la evaluación del riesgo es la identificación de los objetivos a los distintos niveles, vinculados entre sí e internamente

coherentes. La evaluación de los riesgos consiste en la identificación y el análisis de los riesgos relevantes para la consecución de los objetivos, y sirve de base para determinar cómo han de ser gestionados los riesgos. Debido a que las condiciones económicas, industriales, legislativas y operativas continuarán cambiando continuamente, es necesario disponer de mecanismos para identificar y afrontar los riesgos asociados con el cambio.

c) Procedimientos de control

“Se refieren a los procedimientos y políticas adicionales al ambiente de control y al sistema contable establecidos por la gerencia para proporcionar seguridad razonable de lograr los objetivos de la entidad”. (14:73)

d) Información y comunicación

Se debe identificar, recopilar y comunicar información pertinente en forma y plazo que permitan cumplir a cada empleado con sus responsabilidades. Los sistemas informáticos producen informes que contienen información operativa, financiera y datos sobre el cumplimiento de las normas que permite dirigir y controlar el negocio de forma adecuada.

e) Supervisión o monitoreo

Los sistemas de control interno requieren supervisión, es decir, un proceso que comprueba que se mantiene el adecuado funcionamiento del sistema a lo largo del tiempo. Esto se consigue mediante actividades de supervisión continuada, evaluaciones periódicas o una combinación de ambas cosas. La supervisión continuada se da en el transcurso de las operaciones. Incluye tanto las actividades normales de dirección y supervisión, como otras actividades llevadas a cabo por el personal en la realización de sus funciones. El alcance y la frecuencia de las evaluaciones periódicas dependerán esencialmente de una evaluación de los riesgos y de la eficacia de los procesos de supervisión continuada. Las deficiencias detectadas en el control interno deberán ser notificadas a niveles superiores, mientras que

la alta dirección y el consejo de administración deberán ser informados de los aspectos significativos observados.

El control interno informático

Controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la dirección de la organización y/o la dirección informática, así como los requerimientos legales.

La función del control interno informático es asegurarse de que las medidas que se obtienen de los mecanismos implantados por cada responsable sean correctas y válidas.

El control interno informático suele ser un órgano staff de la dirección del departamento de informática y está dotado de las personas y medios materiales proporcionados según los objetivos que se le encomienden.

Como principales objetivos se puede indicar los siguientes:

- a) Controlar que todas las actividades se realicen cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- b) Asesorar sobre el conocimiento de las normas.
- c) Colaborar y apoyar el trabajo de auditoría informática, así como de las auditorías externas al grupo.
- d) Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los niveles adecuados del servicio informático, lo cual no debe considerarse como que la implantación de los mecanismos de medida y responsabilidad del logro de esos niveles se ubique exclusivamente en la función de control interno, si no que cada responsable de objetivos y recursos es responsable de esos niveles, así como de la implantación de los medios de medida adecuados.

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informático salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

El control interno informático controla diariamente que todas las actividades de los sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la dirección de la organización y/o la dirección informática, así como los requerimientos legales.

La función del control interno informático es asegurarse de que las medidas que se obtienen de los mecanismos implantados por cada responsable sean correctas y válidas.

Los controles internos se clasifican en los siguientes:

- a) Controles preventivos: para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.
- b) Controles defectivos: cuando fallan los preventivos para tratar de conocer cuanto antes el evento. Por ejemplo, el registro de intentos de acceso no autorizados, el registro de la actividad diaria para detectar errores u omisiones.
- c) Controles correctivos: facilitan el regreso a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un fichero dañado a partir de las copias de seguridad.

1.2.8 El contador público y auditor como auditor interno

Sin duda alguna, el papel del auditor interno dentro de las organizaciones latinoamericanas, ha evolucionado en la misma medida en que éstas instituciones se han desarrollado.

Es justamente aquel personaje llamado "Auditor Interno", investido con facultades propias de unidades contraloras, revisoras y de consultoría interna quien debe velar por el cumplimiento de las normas y procedimientos corporativos, e ir un poco más allá en la planificación, diseño y realización de sus pruebas de auditoría; enfocando su trabajo no solo a evaluar control interno y emitir su opinión sobre la razonabilidad de los estados financieros en conjunto, se trata pues de evaluar el cumplimiento de las directrices y estrategias emitidas por la alta gerencia, determinando aquellas desviaciones en el cumplimiento de las mismas que pudieran acarrear "Riesgos Asociados" que afecten la capacidad de generación de valor del negocio en el largo plazo.

a) Conocimientos que debe poseer: los auditores internos deben reunir los conocimientos, las aptitudes y otras competencias necesarias para cumplir con sus responsabilidades individuales.

b) Los conocimientos, las aptitudes y otras competencias es un término colectivo que se refiere a la aptitud profesional requerida al auditor interno para llevar a cabo eficazmente sus responsabilidades profesionales. Se alienta a los auditores internos a demostrar su aptitud obteniendo certificaciones y calificaciones profesionales apropiadas, tales como la designación de auditor interno certificado y otras designaciones ofrecidas por el Instituto de Auditores Internos y otras organizaciones profesionales apropiadas.

Se necesitan diversos niveles de conocimiento de tecnología de información en el departamento de auditoría interna para proporcionar un enfoque sistemático y disciplinado a fin de evaluar y mejorar la efectividad de los procesos sobre la gestión de riesgos, los controles y la dirección. El conocimiento de cómo se utiliza tecnología de información, los riesgos relacionados y la capacidad de utilizar la tecnología como un recurso en el desarrollo del trabajo de auditoría interna es esencial para la eficacia del auditor interno en todos los niveles.

El conocimiento de la tecnología de información abarca entender conceptos, como las diferencias en el software usado en aplicaciones, sistemas operativos y software de sistemas y redes. Esto implica entender los componentes básicos de seguridad de la tecnología de información y de control, tales como seguridad perimetral, detección de intrusos, autenticación y controles de los sistemas de aplicación.

El conocimiento básico incluye entender cómo los controles de negocio y los objetivos de aseguramiento pueden verse afectados por vulnerabilidades en las operaciones de negocio y lo relacionado con los sistemas de soporte y los componentes de redes y datos. Es fundamental asegurar que los auditores internos tienen suficiente conocimiento para centrarse en el entendimiento de los riesgos de la tecnología de la información, sin necesariamente tener conocimientos técnicos significativos.

El Contador Público y Auditor, como auditor interno debe contar los conocimientos, aptitudes y competencias necesarias para cumplir con sus responsabilidades como tal.

Los conocimientos se pueden adquirir a través de:

La formación académica, que la brinda una licenciatura, un técnico, posgrado, ya sea administración, finanzas, informática, derecho y legislación tributaria..

La formación complementaria, la cual se da por medio de conferencias, talleres, debates, seminarios, foros, cursos, convenciones y otros.

Y la formación empírica, ésta resulta a lo largo de la carrera profesional del auditor conforme la práctica que desempeña, entre las que se pueden mencionar serían: finanzas, costos, liderazgo, sistemas, procedimientos, legal, fiscal y comercio.

Las tres formaciones anteriores aportan elementos necesarios para la madurez del juicio del auditor interno para realizar su trabajo de manera exitosa, a la fecha por los cambios constantes de la tecnología es forzoso que el auditor interno complemente sus conocimientos informáticos de manera que pueda fortalecer y conocer lo siguiente:

- a) Amenazas y vulnerabilidades relacionadas a procesos automatizados de negocio.
- b) Entender los controles de negocio y la mitigación del riesgo que debe ser proporcionada por la tecnología de información (TI).
- c) Enfoque de planificación y supervisión para las tareas de control interno para considerar las vulnerabilidades y los controles relacionados con la tecnología de información (TI).
- d) Uso de herramientas de tecnología de la información en los trabajos de control interno.

CAPÍTULO II

ÁREA DE CUENTAS POR COBRAR

2.1 CUENTAS POR COBRAR

Son derechos exigibles provenientes de ventas, servicios prestados, préstamos o anticipos otorgados o cualquier concepto documentado con facturas o documentos de crédito.

2.1.1 Definición

Las cuentas por cobrar son derechos legítimamente adquiridos por la empresa que, llegando el momento de ejecutar o ejercer ese derecho, recibirá a cambio efectivo. Las cuentas por cobrar representan derechos exigibles originados por ventas, servicios prestados o cualquier otro concepto análogo. Las ventas al crédito, que originan las cuentas por cobrar, incluyen condiciones de crédito que estipulan el pago dentro de un número determinado de días y se cobra dentro de un periodo menor de un año, lo cual trae como consecuencias que se consideren como activos corrientes de la empresa. Gran parte de las empresas comerciales encuentran que las cuentas por cobrar representan un rubro importante dentro de sus activos corrientes. Esto es motivo suficiente para brindarles atención y tratar de hacer más eficiente la administración de las cuentas por cobrar.

2.1.2 Clasificación

Las cuentas por cobrar pueden clasificarse como de exigencia inmediata:

- a) **Corto plazo:** aquellas cuya disponibilidad es inmediata dentro de un plazo no mayor de un año.
- b) **Largo plazo:** su disponibilidad es a más de un año.

Clasificación de las cuentas por cobrar según NIIF para PYMES:

- ✓ Deudores comerciales y otras cuentas por cobrar: son aquellas que muestren por separado importes por cobrar de partes relacionadas,

importes por cobrar de terceros y cuentas por cobrar procedentes de ingresos acumulados (o devengados) pendientes de facturar.

2.1.3 Naturaleza

Para determinar la naturaleza de la cuenta de cliente, no se tiene que perder de vista el tipo de negocio (unidad de análisis), al ser una empresa de transporte terrestre, el nacimiento de la cuenta de clientes se da en el giro del negocio o sea en las transacciones que se realizan con otras entidades o empresas privadas o individuales así como a personas particulares que requieren sus servicios.

Las cuentas por cobrar provenientes de ventas al crédito, son comúnmente conocidas como “cuentas por cobrar comerciales” o “cuentas por cobrar a clientes” y deben ser presentadas en el balance de situación financiera en el grupo de activo circulante o corriente, excepto aquellas cuyo vencimiento sea mayor que el ciclo normal de operaciones de la empresa, el cual, en la mayoría de los casos es de doce meses.

Cuando el ciclo de operaciones de una empresa es superior a un año y que, como se comentó anteriormente, este hecho permite presentar dentro del activo circulante cuentas por cobrar con vencimiento mayor de doce meses, es necesario que éstas aparezcan separadas de las que vencerán antes de un año. Si se hace caso omiso de esta norma y se separan ambos grupos en una sola cuenta, este hecho debe ser revelado mediante notas al balance de situación financiera.

2.1.4 Registro contable

Ejemplo, el negocio adquiere una cuenta por cobrar cuando vende a clientes mercancías y servicios, a crédito. El término por cobrar significa la promesa del cliente de pagar en una fecha futura, con dinero, el importe que le fue cargado por mercancías o servicios. Por lo general, en los negocios esta promesa se expresa con un importe de efectivo que se cobrará dentro de los próximos 30 días.

Para registrar la venta de una mercancía o servicio a crédito, se hace un cargo a cuentas por cobrar y se acredita una cuenta de ventas o servicios.

Cuando se hace una venta a crédito, lo usual es extender al cliente una factura o comprobante de venta. Con una copia de la factura o comprobante de venta, se anota la operación en los registros contables.

En otras palabras se puede decir que las cuentas por cobrar son, al igual que cualquier activo, recursos económicos propiedad de una empresa que le generarán un beneficio en el futuro. Forman parte del activo circulante.

Las principales cuentas por cobrar son las siguientes: clientes: son las entidades que deben a la empresa por haberles vendido mercancías a crédito, sin exigirles especial garantía documental.

Documentos por cobrar: son títulos de crédito a favor de la empresa, tales como las letras de cambio y pagarés.

Deudores diversos: son las entidades que deben a la empresa por concepto distinto al de venta de mercancías. Funcionarios y empleados: consiste en los préstamos que otorga la empresa a funcionarios y empleados que forman parte de la misma, y se encuentran a su favor.

Las cuentas por cobrar pueden clasificarse de acuerdo con:

- a) Su disponibilidad como de exigencia inmediata o a corto plazo y a largo plazo.
- b) Según su origen, las cuentas por cobrar se clasifican como a cargo de clientes o a cargo de otros deudores como accionistas, funcionarios, empleados, otros.

Las cuentas por cobrar a compañías tenedoras, subsidiarias, afiliadas y asociadas deberán presentarse por separado debido a que presentan características

peculiares en cuanto a su exigibilidad. Los saldos acreedores en las cuentas por cobrar deben clasificarse como cuentas por pagar si su importancia lo amerita. En el caso de que un considerable monto de cuentas por cobrar a cargo de una sola entidad, debe informarse dentro del rubro de cuentas por cobrar o a través de una nota a los estados financieros.

En el caso de que existan cuentas por cobrar y por pagar a cargo de una misma entidad éstas deberán compensarse. Si algunas cuentas o documentos por cobrar están en moneda extranjera deben informarse en el cuerpo del balance de situación financiera o mediante una nota a los estados financieros.

Es importante señalar que las cuentas por cobrar generalmente se encuentran en el corto plazo, es decir, elementos o partidas convertibles en efectivo en un plazo menor de doce meses. Dentro de esta clasificación, se encuentran las cuentas mencionadas anteriormente: clientes, documentos por cobrar, deudores diversos, funcionarios y empleados, plazos de las cuentas por cobrar.

Las cuentas por cobrar son un aspecto muy significativo para cualquier organización, ya que éstas representan ingresos. El objetivo de administrar las cuentas por cobrar es cobrarlas tan rápido como sea posible sin perder ventas debido a técnicas de cobranza muy agresivas. El logro de esta meta comprende tres temas: selección y estándares de crédito, condiciones de crédito, supervisión de crédito.

Supervisión de crédito. Es el aspecto final que una empresa debe considerar en su administración de las cuentas por cobrar. La supervisión del crédito es una revisión continua de las cuentas por cobrar de la organización para determinar si los clientes están pagando conforme a las condiciones de crédito establecidas. En esta fase, las empresas utilizan diversas técnicas populares de cobro: cartas, llamadas telefónicas, visitas personales, agendas de cobro, acción legal.

Cartas: después de cierto número de días, la empresa envía una carta formal que sirve como recordatorio al cliente. Llamadas telefónicas: si las cartas no tienen éxito, se puede realizar una llamada telefónica para avisar al cliente sobre el pago inmediato.

Visitas personales: consiste en enviar a un vendedor local para confrontar al cliente.

Agencias de cobro: las empresas pueden remitir las cuentas incobrables a una agencia de cobro o un abogado de cobranzas.

Acción legal: es el paso más severo y una alternativa para el uso de una agencia de cobro.

2.1.5 Presentación en los estados financieros

Las cuentas por cobrar su presentación en los estados financieros deben hacerse en la sección del activo corriente del estado de situación financiera.

2.1.6 Cuentas incobrables

Son aquellas que por alguna razón se estiman de cobro difícil, normalmente se refiera a las de clientes. Saldo pendiente de una obligación de crédito que una institución de préstamo ya no tiene esperanza de recuperar y que pasa a pérdidas.

Es el derecho que tiene el vendedor sobre el comprador por el importe de la operación, son derechos monetarios contra negocios y personas.

✓ Causas

La mayor parte de las ventas se realizan a crédito, en muchos casos respaldadas por facturas que están registradas dentro de las "cuentas por cobrar" Si se hace imposible el cobro de algunas de estas facturas (quiebra del cliente, muerte o cambio de domicilio del mismo) se debe

que traspasarlas a los gastos del ejercicio, ya que la incobrabilidad de las mismas constituye una pérdida para el negocio.

“Las ventas a crédito se registran como ingreso del ejercicio donde se producen, por lo que cuando se producen pérdidas por cuentas por cobrar (por las ventas a crédito que se convierten en incobrables) se deben registrar dentro del mismo ejercicio. Generalmente en la fecha de cierre no se tiene la certeza de cuáles facturas se perdieron definitivamente y como hay que registrar la pérdida de cuentas por cobrar por posible incobrabilidad hay que proceder a hacer una estimación sobre las posibles pérdidas (lo más adaptado a la realidad que se pueda) y crear una cuenta de provisión para absorber esas posibles pérdidas.

En la fecha de cierre se hace la estimación de las posibles pérdidas y se cargan a una cuenta de gasto llamada "pérdida en cuentas incobrables" que se incluye dentro de los gastos de Operación en el estado de resultados, y la estimación se abona en el asiento a una cuenta de valoración" (26:1).

Las cuentas incobrables, enfoque tributario, conforme al artículo 21 numeral 20 de la ley de actualización tributaria, Decreto 10-2012, son deducibles de la renta obtenida por el contribuyente que opera en el régimen sobre las utilidades de actividades lucrativas, las cuentas incobrables que se originen en operaciones del giro habitual del negocio o la imputación realizada a una reserva que no podrá exceder del tres por ciento (3%) de los saldos deudores de cuentas y documentos por cobrar al cierre de cada uno de los periodos anuales de liquidación.

Dichas formas de deducción son alternativas, pudiendo el contribuyente elegir entre una u otra.

Una vez elegida la forma de deducción directa o la de reserva, ésta solamente puede ser cambiada con autorización expresa y previa de la administración

tributaria y sólo en los casos que se justifique la necesidad del cambio. En los casos que se autorice el cambio, éste tendrá efecto en el período de liquidación definitiva anual inmediato siguiente a aquél de su autorización.

Si al final del período anual de imposición la reserva creada y la respectiva imputación al gasto fue declarado como deducible en algún período anterior, excede al tres por ciento (3%) del saldo principal de cuentas y documentos por cobrar, el contribuyente imputará la diferencia a la renta bruta del período de liquidación correspondiente.

2.1.7 Normas internacionales de contabilidad (NIC)

“Estas normas han sido producto de grandes estudios y esfuerzos de diferentes entidades educativas, financieras y profesionales del área contable a nivel mundial, para estandarizar la información financiera presentada en los estados financieros.

Las NIC, como se le conoce popularmente, son un conjunto de normas o leyes que establecen la información que deben presentarse en los estados financieros y la forma en que esa información debe aparecer, en dichos estados. Las NIC no son leyes físicas o naturales que esperaban su descubrimiento, sino más bien normas que el hombre, de acuerdo a sus experiencias comerciales, ha considerado de importancia en la presentación de la información financiera.

Son normas de alta calidad, orientadas al inversor, cuyo objetivo es reflejar la esencia económica de las operaciones del negocio, y presentar una imagen fiel de la situación financiera de una empresa. Las NIC son emitidas por el International Accounting Standards Board (anterior International Accounting Standards Committee). Hasta la fecha, se han emitido 41 normas, de las que 34 están en vigor en la actualidad, junto con 30 interpretaciones”. (3:1)

2.1.8 Marco conceptual

El marco conceptual para la preparación de los estados financieros establece los principios básicos para las NIC. El marco conceptual establece los objetivos de los estados financieros y proporciona información acerca de la posición financiera, rendimiento y cambios en la posición financiera de la entidad que es útil para que un amplio rango de usuarios puedan tomar decisiones.

✓ Elementos de los estados financieros

La situación financiera de una entidad es la relación entre los activos, los pasivos y el patrimonio en una fecha concreta, tal como se presenta en el estado de situación financiera. Estos se definen como sigue:

- a. Un activo es un recurso controlado por la entidad como resultado de sucesos pasados, del que la entidad espera obtener, en el futuro, beneficios económicos.
- b. Un pasivo es una obligación presente de la entidad, surgida a raíz de sucesos pasados, al vencimiento de la cual, espera desprenderse de recursos que incorporan beneficios económicos.
- c. Patrimonio es la parte residual de los activos de la entidad, una vez deducidos todos sus pasivos.

✓ Contenido de los estados financieros

Un conjunto completo de estados financieros incluyen lo siguiente según las NIIF para PYMES, en su sección 3.17:

- a. Un estado de situación financiera a la fecha sobre la que se informa.
- b. Una u otra de las siguientes informaciones:
 - i. Un solo estado del resultado integral para el periodo sobre el que se informa que muestre todas las partidas de ingresos y gastos reconocidas durante el periodo incluyendo aquellas partidas reconocidas al determinar el resultado (que es un subtotal en el estado del resultado integral) y las partidas de otro resultado integral.

- ii. Un estado de resultados separado y un estado del resultado integral separado. Si una entidad elige presentar un estado de resultados y un estado del resultado integral, el estado del resultado integral comenzará con el resultado y a continuación, mostrará las partidas de otro resultado integral.
- c. Un estado de cambios en el patrimonio del periodo sobre el que se informa.
- d. Un estado de flujos de efectivo del periodo sobre el que se informa.
- e. Notas, que comprenden un resumen de las políticas contables significativas y otra información explicativa.

CAPÍTULO III

SISTEMAS INFORMÁTICOS Y PROCEDIMIENTOS DE CONTROL INTERNO EN LA PREVENCIÓN DE FRAUDES EN EL ÁREA DE CUENTAS POR COBRAR

3.1 SISTEMA DE INFORMACIÓN COMPUTARIZADA

La informática es la disciplina que se dedica a estudiar la información y sus componentes, así como la tecnología para manejarla, conservarla y utilizar de manera eficiente y económica, con miras a facilitar su acceso a otras personas para producir mayores beneficios.

3.1.1 Definición

Es un soporte informático, es decir se desarrollan en un entorno usuario-computadora, utilizando hardware y software, redes de telecomunicaciones, técnicas de administración de base de datos.

3.1.2 Aplicación

Las solicitudes de sistemas de información están motivadas por los siguientes objetivos generales:

- a) **Resolver un problema:** actividades procesos o funciones que en la actualidad o quizás en el futuro, no satisfacen los estándares de desempeño o las expectativas para lo que es necesario emprender una acción que resuelva las dificultades.
- b) **Aprovechar una oportunidad:** para ampliar o mejorar el rendimiento económico de la empresa y su competitividad dentro del mercado.
- c) **Responder:** proporcionar información en respuesta a órdenes, solicitudes o mandatos originados por una autoridad legislativa o administrativa, llevar a cabo tareas de cierta manera, o también cambiar la información o tal vez el desempeño.
- d) **Obtener capacidad:** las actividades de la organización están influenciadas por la capacidad de ésta, para procesar transacciones con rapidez y eficiencia.

- e) **Obtener procesamientos acelerados:** la velocidad inherente con que la computadora procesa datos es una de las razones por las que las organizaciones buscan el desarrollo de proyectos. Los sistemas basados en computadoras pueden ser de ayuda para eliminar la necesidad de cálculos tediosos y comparaciones repetitivas.
- f) **Obtener aumento en volumen:** dado que los sistemas de información constituyen una ventaja para la compañía es frecuente que reciban una consideración primaria antes o durante el crecimiento y ampliación de la empresa. La incapacidad para mantener el ritmo de procesamiento no necesariamente significa el abandono de los procedimientos existentes.
- g) **Obtener información rápida:** las organizaciones almacenan grandes cantidades de datos relacionados con sus operaciones, empleados, clientes, proveedores y finanzas.

3.1.3 Seguridad

La importancia de la seguridad de la información es un elemento de significativa y creciente preocupación en las organizaciones modernas y constituye un activo altamente apreciable que puede hacer la diferencia entre el éxito y el fracaso de una organización.

- ✓ **La importancia de la seguridad de los sistemas contables informáticos**
"La seguridad de la información se ha convertido en uno de los temas más importantes en la mayoría de las organizaciones desde que la supervivencia y éxito de las mismas depende, en gran medida, en la confidencialidad, exactitud, integridad y disponibilidad de los datos que manejan.
- ✓ **Los componentes de la seguridad**
 - a. Seguridad física: la seguridad de los sistemas de información envuelve la protección de la información así como la de los sistemas computacionales. También está involucrada en esta sección la seguridad

del equipamiento adicional necesario y las personas designadas al manejo de la información.

- b. Seguridad de datos: los datos son el corazón de los sistemas informáticos por tanto estos deben ser celosamente cuidados y manejados.

3.1.4 Humanware

El concepto Humanware se utiliza para resaltar la importancia del lado Humano de la interacción entre los principales actores involucrados en los procesos de reestructuración, reingeniería y modernización empresarial para garantizar el éxito incorporación de nuevas tecnologías en hardware o software y demás servicios requeridos, de un lado entre productores, proveedores con su equipo de mercadeo, ventas, educación y servicios de apoyo y del otro lado con empresas compradoras de soluciones en informática y telecomunicaciones a través de las áreas funcionales del negocio, tales como sistemas, servicio al cliente, finanzas, producción y usuarios primarios o finales.

3.1.5 Software

Deriva de la raíz soft cuya traducción es "blanda o suave". Con este término se abarca a toda la parte lógica, al conjunto de programas que se puede ejecutar en una computadora. Software es todo aquello que puede modificarse: programas y datos, que pueden estar grabados o cambiar día a día. Por ejemplo: los sistemas operativos, los graficadores, las planillas de cálculo, otros.

✓ Clasificación

El software se clasifica en 3 diferentes categorías: sistemas operativos, lenguajes de programación y software de aplicación.

✓ Sistemas operativos

El sistema operativo es el gestor y organizador de todas las actividades que realiza la computadora. Marca las pautas según las cuales se intercambia

información entre la memoria central y la externa, y determina las operaciones elementales que puede realizar el procesador. El sistema operativo, debe ser cargado en la memoria central antes que ninguna otra información.

✓ **Sistema operativo SQL**

“Es un sistema de gestión de bases de datos relacional, contenida en una relativamente pequeña biblioteca escrita, es un proyecto de dominio público creado por D. Richard Hipp.” (18:1)

A diferencia de los sistemas de gestión de bases de datos cliente-servidor, el motor de SQL no es un proceso independiente con el que el programa principal se comunica. En lugar de eso, la biblioteca SQL se enlaza con el programa pasando a ser parte integral del mismo. El programa utiliza la funcionalidad de a través de llamadas simples a subrutinas y funciones. Esto reduce la latencia en el acceso a la base de datos, debido a que las llamadas a funciones son más eficientes que la comunicación entre procesos. El conjunto de la base de datos (definiciones, tablas, índices, y los propios datos), son guardados como un sólo fichero estándar en la máquina host (huésped). Este diseño simple se logra bloqueando todo el fichero de base de datos al principio de cada transacción.

✓ **Lenguajes de programación**

Mediante los programas se indica a la computadora que tarea debe realizar y cómo efectuarla, pero para ello es preciso introducir estas órdenes en un lenguaje que el sistema pueda entender.

En principio, el ordenador sólo entiende las instrucciones en código máquina, es decir, el específico de la computadora. Sin embargo, a partir de éstos se elaboran los llamados lenguajes de alto y bajo nivel.

✓ **Base de datos visual basic**

“Visual Basic es un lenguaje de programación dirigido por eventos, desarrollado por Alan Cooper para Microsoft. Este lenguaje de programación es un dialecto de BASIC, con importantes agregados. Su primera versión fue presentada en 1991, con la intención de simplificar la programación utilizando un ambiente de desarrollo que facilitó en cierta medida la programación misma”. (18:1)

✓ **Bases de datos**

“Es un banco de datos o un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido; una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta. Actualmente y debido al desarrollo tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos están en formato digital (electrónico) y por ende se ha desarrollado y se ofrece un amplio rango de soluciones al problema del almacenamiento de datos”. (18:1)

✓ **Software de aplicación**

“El software de aplicación está diseñado y escrito para realizar tareas específicas personales, empresariales o científicas como el procesamiento de nóminas, la administración de los recursos humanos o el control de inventarios. Todas éstas aplicaciones procesan datos (recepción de materiales) y generan información (registros de nómina), para el usuario”. (18:1)

3.1.6 Hardware

“Son todos los dispositivos y componentes físicos que realizan las tareas de entrada y salida”. (18:1)

Según NIA 240 lo define como un acto intencionado realizado por una o más personas de la dirección, los responsables del gobierno de la entidad, los empleados o terceros, que conlleve la utilización del engaño con el fin de conseguir una ventaja injusta o ilegal.

✓ **Características del fraude**

Según NIA 240 establece que, las incorrecciones en los estados financieros pueden deberse a fraude o error. El factor que distingue el fraude del error es que la acción subyacente que da lugar a la incorrección de los estados financieros sea o no intencionada.

Aunque "fraude" es un concepto jurídico amplio, a los efectos de las NIA al auditor le concierne el fraude que da lugar a incorrecciones materiales en los estados financieros. Para el auditor son relevantes dos tipos de incorrecciones intencionadas: las incorrecciones debidas a información financiera fraudulenta y las debidas a una apropiación indebida de activos. Aunque el auditor puede tener indicios o, en casos excepcionales, identificar la existencia de fraude, el auditor no determina si se ha producido efectivamente un fraude desde un punto de vista legal.

3.2.2. Definición

"El delito informático implica cualquier actividad ilegal que encuadra en figuras tradicionales ya conocidas como robo, hurto, fraude, falsificación, perjuicio, estafa y sabotaje, pero siempre que involucre la informática de por medio para cometer la ilegalidad". (18:1)

3.2.3 Origen

"Limitar el fraude informático a los actos fruto de la intencionalidad, realizados con la voluntad de obtener un beneficio propio y si es posible, provocar un perjuicio a alguien. Así, se puede hablar también de un tipo de fraude informático no intencionado, producto de un error humano al utilizar un sistema informático o por un defecto del hardware o el software. Este tipo de fraude es conocido como "error informático". En el caso del error informático puede no haber un beneficio directo

para quien causa el funcionamiento erróneo del sistema informático, pero sí un perjuicio a los otros usuarios o a los propietarios del sistema". (18:1)

3.2.4 Daños o modificaciones de programas o datos computarizados

Son los daños que realizan a los programas a los siguientes elementos:

✓ **Sabotaje informático**

"Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema". (18:1)

✓ **Virus**

"Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya. (software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado)". (18:1)

✓ **Gusanos**

"Se fabrica en forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus; por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema para que transfiera continuamente dinero a una cuenta ilícita". (18:1)

✓ **Bomba lógica o cronológica.**

“Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar donde se halla la bomba”. (18:1)

✓ **Acceso no autorizado a servicios y sistemas informáticos.**

“Es el acceso no autorizado a sistemas informáticos por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático”. (18:1)

3.2.5 Clasificación

✓ **La manipulación indebida de datos a través de la utilización de un sistema de tratamiento de la información**

- a) Como objeto: alteración de los datos digitales.
- b) Como instrumento: uso de las computadoras para falsificar documentos de uso comercial.
- c) Los daños o modificaciones de programas o datos computarizados.
- d) Acceso no autorizado a servicios y sistemas informáticos.
- e) Reproducción no autorizada de programas informáticos de protección legal.

✓ **Espionaje informático**

“Los programas de espionaje informático envían informaciones del computador del usuario de la red para desconocidos. Hasta lo que es digitado en su teclado puede ser monitoreado por ellos. Algunos tienen un mecanismo que hace una conexión con el servidor del usuario siempre que él estuviera conectado on-line”. (18:1)

Existen diferentes técnicas para realizar este tipo de espionaje informático, entre ellas:

- a) **Dialers:** es la instalación de un marcador que provoca que la conexión a Internet se realice a través de un número de tarificación especial y no a través del modo indicado por el operador con el que se haya contratado dicha conexión.
- b) **Adware:** son programas que recogen o recopilan información acerca de los hábitos de navegación del usuario en cuestión.
- c) **Programas de acceso remoto:** que permiten el acceso de un tercero a su ordenador para un posterior ataque o alteración de los datos. Son fácilmente reconocibles por los antivirus.
- d) **Caballos de Troya:** este programa es conocido ya que una vez instalado en el ordenador provoca daños o pone en peligro la seguridad del sistema.
- e) **Virus o gusanos (worms):** es un programa o código que provoca daños en el sistema, como alteración o borrado de datos, se propaga a otros computadores haciendo uso de la Red, del correo electrónico, otros.
- f) **Programas de espionaje o spyware:** es un programa que se encarga en registrar todo lo que se realiza en un PC, hasta un sencillo 'clic' en el ratón queda almacenado. Se utiliza para obtener información confidencial o conocer cuál es el funcionamiento que una persona le está dando a la máquina.

✓ **Sabotaje informático**

El sabotaje informático, es el acto de borrar, suprimir o modificar sin autorización funciones o datos del sistema informático (hardware y/o software) con intención de obstaculizar el funcionamiento normal del sistema.

✓ **Piratería**

“La piratería que, como es sabido, comenzó con los orígenes de la navegación y se practicó por todos los mares del globo terráqueo, y aun se practica en algunos, no podía dejar fuera de su campo de acción a uno de los mares por donde navega uno de los mayores tráficos comerciales de la actualidad: Internet”. (18:1)

✓ **Hacking**

“Cuando se habla sobre “Hacking” o se menciona la palabra “Hacker” normalmente se suele pensar en alguien que tiene profundos conocimientos sobre máquinas que realizan funciones de cómputo y que, además son personas que realizan cosas imposibles para el resto de mortales, habitualmente también se relacionan con personas que se dedican a realizar estafas a gran escala sobre bancos y/o grandes multinacionales, eso para la sociedad moderna, es un hacker”(18:1).

✓ **Phishing**

“El término **Phishing** se refiere a uno de los métodos más usados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima”. (18.1)

El estafador, conocido como phisher, se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea, redes sociales SMS/MMS, a raíz de un malware o incluso utilizando también llamadas telefónicas.

Distinguir un mensaje de phishing de otro legítimo puede no resultar fácil para un usuario que haya recibido un correo de tales características,

especialmente cuando es efectivamente cliente de la entidad financiera de la que supuestamente proviene el mensaje.

El campo del mensaje muestra una dirección de la compañía en cuestión. No obstante, es sencillo para el estafador modificar la dirección de origen que se muestra en cualquier cliente de correo.

El mensaje de correo electrónico presenta logotipos o imágenes que han sido recogidas del sitio web real al que el mensaje fraudulento hace referencia.

El enlace que se muestra parece apuntar al sitio web original de la compañía, pero en realidad lleva a una página web fraudulenta, en la que se solicitarán datos de usuarios, contraseñas, otros.

Normalmente estos mensajes de correo electrónico presentan errores gramaticales o palabras cambiadas, que no son usuales en las comunicaciones de la entidad por la que se están intentando hacer pasar.

3.2.6 Factores que facilitan el fraude

Así como existen motivos, también existen factores que facilitan e inducen al fraude o el engaño, el principal es pensar que nunca nos van a atrapar. Dicho lo anterior, la primera regla para evitar el fraude o el engaño es tomar medidas para prevenirlo.

3.2.7 Clasificación del fraude en Auditoría

De acuerdo a la asociación de examinadores de fraude-ACFE- por sus siglas en idioma inglés las siguientes modalidades de fraude. Este tipo de fraude se efectúa en los documentos de la empresa.

- a) Manipulación de registros.
- b) Manipulación de documentos.

- c) Destrucción de documentos.
- d) Alteración de documentos legítimos.
- e) La ocultación de documentos.
- f) Firmas responsables en soporte no verificadas.
- g) Adulteración de comprobantes.
- h) Atraso en los registros contables.
- i) Notas de crédito emitidas no autorizadas.

3.2.8 Tipos de fraude

“Se considera que hay dos tipos de fraude: el primero de ellos se realiza con la intención financiera clara de malversación de activos de la empresa. El segundo tipo de fraude, es la presentación de información financiera fraudulenta como acto intencionado encaminado a alterar las cuentas anuales.

- a) Los fraudes denominados internos son aquellos organizados por una o varias personas dentro de una institución, con el fin de obtener un beneficio propio.
- b) Los fraudes conocidos como externos son aquellos que se efectúan por una o varias personas, clientes, proveedores, otros.”. (18:1)

3.2.9 Técnicas para realizar fraudes electrónicos

“Existen múltiples técnicas para perpetrar fraudes económicos a través de Internet, pero sin duda, una de las técnicas que está obteniendo importantes índices de crecimiento en la red, es la suplantación de páginas y/o sitios de Internet, más conocida como "phishing", que permite al estafador, mediante el engaño, conocer los datos privados y personales que usted utiliza para la realización de operaciones económicas.

Los fraudes por medios electrónicos han crecido exponencialmente en los últimos años. La inminente necesidad de usar Internet como medio de comunicación prioritaria ha abierto la puerta a múltiples estafadores que lo usan como un nuevo

medio para atacar y defraudar a usuarios y empresas por igual. Es importante aprender a defenderse de cualquier tipo de ataques de este tipo, con ciertas medidas de precaución uno puede reducir mucho el riesgo". (18:1)

3.2.10 Fraudes en el área de cuentas por cobrar

Las cuentas por cobrar son altamente vulnerables a fraudes. Las modalidades más comunes en que ocurre el fraude en esta área son la apropiación indebida de fondos, cuentas por cobrar ficticias y registro indebido de notas de crédito.

La apropiación indebida de fondos, una modalidad bastante común, consiste en utilizar ciertas entradas de dinero para sustituir otras entradas previamente desviadas, postergando así la detención del robo.

3.2.11 Prevención del fraude en las cuentas por cobrar

"Un programa de prevención y detección del fraude debe contar con tres componentes básicos:

1. Un código de ética, una política de fraude formal y políticas y procedimientos operativos que apoyen actividades para la prevención de fraude.
2. Un programa educativo de concientización e identificación del fraude que abarque cuando menos los niveles gerenciales de la compañía.
3. Un sistema de monitoreo de posibles violaciones al código de ética y de identificación de posibles fraudes dentro de la empresa. En la práctica, estos componentes tienen elementos tanto de prevención como de detección, y contribuyen al logro de ambos objetivos simultáneamente". (56:1)

Para prevenir fraudes se debe tomar en cuenta los indicadores siguientes:

- ✓ Determinar líneas claras de responsabilidad y autoridad.
- ✓ Implementación de metas operativas realistas.

- ✓ Diseñar políticas y procedimientos de personal uniformes, claros y precisos sobre: conducta laboral, ética de negocios y conflicto de intereses.
- ✓ Prácticas de compensación altas.
- ✓ Comunicación al personal sobre las reglas y acciones tomadas para combatir el fraude y actos deshonestos.
- ✓ Castigo a los infractores.
- ✓ Programa de entrenamiento adecuado para el personal.
- ✓ Controlar las transacciones con partes relacionadas e inusuales.
- ✓ Sistema y ambiente de control interno rigurosos.
- ✓ Control de documentos para evitar su alteración.
- ✓ Evitar cheques con dos endosos.
- ✓ Evitar documentos soportes.
- ✓ Utilizar documentos originales.
- ✓ No permitir correcciones con corrector y tachaduras.
- ✓ Cancelar en su totalidad los documentos ya cobrados o cancelados de cuentas por cobrar.
- ✓ Un riguroso control en el sistema de registro contable y contar con suficiente personal para manejar el nivel de operaciones.
- ✓ Control de las transacciones materiales e inusuales en fecha de cierre contable.
- ✓ Control total y utilizar el menor número de cuentas bancarias, para poder darle seguimiento a todas las operaciones registradas.
- ✓ Controlar si hay apropiación indebida del dinero de una organización antes de que se haya registrado en el sistema contable.
- ✓ Ventas al contado o cuentas a cobrar. Puede ocurrir en cualquier punto: vendedores, cajeros, recepcionistas y otros que reciben dinero directamente de los clientes.
- ✓ Controlar si hay ventas no registradas.
- ✓ No trabajar sin supervisión.
- ✓ Deben de reportar los ingresos periódicamente.

- ✓ Reportar los descuentos y bonificaciones, contabilizando descuentos.
- ✓ Llevar control en las cuentas que son muy grandes o que se encuentran atrasadas y están por ser consideradas incobrables.
- ✓ Control de acreditaciones de una cuenta por medio de la sustracción de dinero de otra cuenta, clientes A, B, C.
- ✓ Adulteración de saldo de cuentas o destrucción de registros de transacción.
- ✓ Control de que existan falsificaciones en los registros para ocultar el hurto de los pagos provenientes de cuentas por cobrar.
- ✓ Control de débitos en cuentas ficticias
- ✓ Mantengan una permanente presencia gerencial en los lugares de venta.
- ✓ Instalar una cámara de video en los sitios de ingreso de dinero.
- ✓ Ubicar las cajas registradoras en grupos de manera que los empleados puedan controlarse entre sí.
- ✓ Eliminar sitios que no estén a la vista, cercanos a las cajas registradoras, que puedan ser utilizados para ocultar el dinero hurtado.
- ✓ Aprender a identificar indicadores cercanos a las cajas registradoras y entrenar a los gerentes para que los busquen.
- ✓ Obligar a los clientes para que requieran recibos por sus compras.
- ✓ Implementar la rotación de funciones y / o horarios de trabajo de los empleados.
- ✓ Requerir a los vendedores en otras localidades un registro que incluya todas, las visitas realizadas y otras actividades de negocios relacionados.
- ✓ Revisar, en forma selectiva, la veracidad de los registros de actividades de los vendedores.
- ✓ Realizar análisis de tendencias de ventas para los vendedores externos.
- ✓ Verificar los reclamos de los clientes en forma independiente del personal de ventas.
- ✓ Verificar siempre que el total de los depósitos coincida con el total contabilizado en las cuentas por cobrar.

- ✓ Buscar ajustes, correcciones y otras alteraciones en los libros. También busque transacciones irregulares contabilizadas en cuentas misceláneas
- ✓ Efectuar el monitoreo de todos los ajustes y/o descuentos buscando patrones por empleados, clientes o importes.
- ✓ Realizar análisis de tendencias buscando cantidades inusuales de cuentas vencidas.
- ✓ Obtener reportes de movimientos de cuentas inactivas identificando débitos en estas cuentas.
- ✓ Realizar, en forma periódica, confirmaciones independientes con los clientes para asegurar que sus registros contables coincidan con los de la organización.
- ✓ Revisar los residuos de la oficina de correspondencia para identificar sobres de confirmaciones a clientes no enviadas.
- ✓ Observar a los empleados que dedican una cantidad importante de horas fuera del horario habitual o durante fines de semana.
- ✓ Hacer cumplir las vacaciones obligatorias.
- ✓ Verificar el área de trabajo y/o residuos en la oficina del sospechoso para identificar anotaciones u otra evidencia documentada.
- ✓ Otro medio efectivo para evitar el robo o fraude es repartir entre dos o tres empleados la tarea de verificar y contabilizar los recibos que ingresan.
- ✓ Otra medida efectiva es investigar en persona los reclamos de clientes que aseguren que no se les ha asignado crédito por concepto de los pagos realizados. Un sello podría ayudar a evitar la falsificación de los documentos.
- ✓ Poner atención a los detalles, un empleado que está malversando fondos debe esforzarse permanentemente por ocultar este tipo de robo. Muchos pequeños empresarios se sorprenden al descubrir que trabajadores que nunca tomaban vacaciones ni se ausentaban por motivos de salud, en realidad les estaban robando, coinciden los expertos. En el caso de un fraude, la razón de esta actitud 'ejemplar' radica en que estos empleados

deben estar permanentemente en la oficina para cubrir todo rastro de sus acciones.

- ✓ Las auditorías, grandes aliadas. Al menos una vez al año, contrata algún despacho externo para que haga una auditoría de la contabilidad de la empresa.
- ✓ Al buen entendedor. Generalmente los fraudes se presentan cuando la contabilidad está desordenada o no tienen ninguna supervisión, lo que permite a un empleado quedarse con efectivo y recibos.

3.3 PROCEDIMIENTOS DE CONTROL INTERNO PARA LA PREVENCIÓN DE FRAUDES INFORMÁTICOS EN EL ÁREA DE CUENTAS POR COBRAR

3.3.1 Definición

Los procedimientos de control interno de una empresa forma parte del control de gestión de tipo práctico y está constituido por el plan de organización, la asignación de deberes y responsabilidades, el sistema de información financiero y todas las medidas y métodos encaminados a proteger los activos, promover la eficiencia, obtener información financiera confiable, segura y oportuna y lograr la comunicación de políticas administrativas y estimular y evaluar el cumplimiento de estas últimas.

3.3.2 Procedimientos de control interno para la organización del área de contabilidad

Uno de los principios del control interno es la segregación de funciones es para prevenir el fraude interno en la organización. Con esto un individuo no llevará a cabo todas las actividades de operación, no todo estará bajo su responsabilidad, ninguna persona debe manejar todas las fases de una transacción "ninguna persona debe ser capaz de registrar, autorizar y conciliar una transacción". Ello como mecanismo de protección para esas mismas personas (ya se trate de empleados o de administradores) y de la misma organización.

Toda transacción debe pasar por las fases de: aprobación, autorización, ejecución y registro, cuyo control debe estar a cargo de empleados independientes del departamento que posee la responsabilidad de la operación.

Esta segregación de funciones se hace para poder detectar errores involuntarios y para que ninguna persona se halle predispuesta a cometer desfalco o fraude sin confabulación con otros empleados.

Todos los cargos deben tener un manual de funciones y procedimientos, aquel documento técnico normativo que los define dentro de la estructura orgánica y funcional de la empresa, allí debe especificarse por puesto únicamente algunas funciones para una parte de la transacción.

A la fecha todas las aplicaciones de software administrativo cuentan con perfiles de usuario restringidos y perfiles máster que permiten limitar el acceso total a una operación económica, más aún así estos "programas" continúan siendo vulnerables y el fraude se sigue cometiendo, todo por no tener una adecuada segregación de funciones.

La administración de la empresa debe optar por incluir restricciones en todos los aplicativos de la empresa, un mismo empleado no debería tener más de dos responsabilidades sobre un software y este tipo de sistemas de manera imprescindible debe tener un monitoreo constante, por el departamento de sistemas o por el mismo control interno de la organización.

Así mismo se debe determinar si la estructura de organización del área de contabilidad es la más apropiada para que éstos funcionen con eficacia y eficiencia en la empresa, lo cual se logra mediante el diseño adecuado de 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 responsabilidad y la definición clara de los perfiles de puestos.

Para este elemento de control interno se proponen los siguientes subelementos:

- a) Dirección
- b) División del trabajo
- c) Asignación de responsabilidad y autoridad
- d) Establecimiento de estándares y métodos
- e) Perfiles de puestos

a) Dirección

Es uno de los subelementos básicos del control interno en cualquier empresa, ya que esta es la función primordial de la entidad o persona que tiene la misión de dirigir la actividades en la institución o en un área específica, así como la de coordinar el uso de los recursos disponibles en el área para cumplir en objetivo institucional. Esto se aplica al control interno de la empresa ya que el titular de la entidad o persona responsable de dirigir el área contable de la empresa tiene la responsabilidad de ejercer la autoridad en la conducción de las funciones y actividades del personal de dicha área, así como en la coordinación de los recursos informáticos que le permitirán satisfacer los requerimientos de sistemas de la empresa, este subelemento permite determinar de manera correcta los niveles de autoridad y responsabilidad que se necesitan en la estructura de organización del área de contabilidad, con el fin de poder supervisar y evaluar el cumplimiento de las funciones y el buen desempeño de las actividades del personal asignado a esos puestos.

Este subelemento estará apoyado por lo siguiente:

- ✓ La coordinación de los recursos. Asignar y distribuir de manera correcta los recursos de contabilidad disponibles en la empresa.

- ✓ La supervisión de actividades. Es la vigilancia sobre la realización adecuada de las funciones y actividades que se tienen encomendadas en esta área.
- ✓ La delegación de autoridad y responsabilidad. Es indispensable hacer una distribución adecuada de los límites de autoridad y responsabilidad en todos los niveles, obligar al personal del área de acuerdo a la delegación de autoridad y responsabilidad a cumplir con las tareas y funciones y operaciones que tienen encomendadas.
- ✓ La asignación de actividades. Definición clara y concreta de todas las funciones, tareas y operaciones de cada puesto.
- ✓ La distribución de recursos. Es la asignación que se hace de los recursos disponibles con el propósito de que los empleados de esta área cumplan eficientemente con las actividades y tareas que tienen encomendadas.

b) División del trabajo

Para el buen desarrollo de las actividades de cualquier empresa es necesario que las actividades se realicen de acuerdo a como hayan sido diseñadas en la estructura de la organización y de acuerdo con lo delimitado por el perfil de puestos. (Se deben distribuir de manera correcta las cargas de trabajo).

La división del trabajo incrementa la eficacia y eficiencia de las actividades de cualquier empresa. Se requiere una división más especializada del trabajo para el cumplimiento de las actividades y operaciones y tareas que se desarrollan.

c) Asignación de responsabilidad y autoridad

Es la asignación de las líneas de autoridad por puesto y el establecimiento de los límites de responsabilidad de las líneas de autoridad por puesto y el establecimiento de los límites de responsabilidad que tendrá cada uno de

estos, incluyendo los canales formales de comunicación. Delimita claramente la autoridad y responsabilidad que tendrá cada integrante de cada área para tener un mejor desarrollo de las actividades, funciones y tareas por lo que el procesamiento de información en la empresa será más eficiente y más eficaz.

d) Establecimiento de estándares y métodos

Es de suma importancia estandarizar el desarrollo de todas las actividades y funciones a fin de que éstas se realicen de manera uniforme conforme a las necesidades concretas de las unidades que integran la empresa. Se deben establecer de manera homogénea y uniforme todos aquellos procedimientos y metodologías que permitan estandarizar la operación, así como para el desarrollo de nuevos sistemas de operación.

e) Perfil de puestos

Este elemento del control interno del departamento contable ayuda a identificar y establecer los requisitos, habilidades, experiencia y conocimientos específicos que necesita tener el personal que ocupa un puesto en esta área. Se debe de considerar dentro del perfil de puestos cada una de las características que deben poseer quienes ocupan los puestos que integran la estructura de organización de la empresa.

Con el perfil de puestos se pretende estandarizar hasta donde es posible, los requisitos mínimos que se deben contemplar para cada uno de los puestos del departamento de contabilidad.

Es trascendental destacar la importancia del uso del perfil de puestos para la selección adecuada del personal que ocupará los puestos dentro del área, debido a que en este documento se establecerán en forma precisa y correcta las características, conocimientos y habilidades que deberán tener

quienes ocupen dichos puestos. Esto será la garantía de un desarrollo eficiente y eficaz de las funciones y actividades de cada puesto.

3.3.3 Procedimientos de control interno en el área de cuentas por cobrar:

- a) El departamento debe estar dirigido por una sola persona.
- b) El otorgamiento de crédito a clientes, funcionarios y empleados se efectuará sobre la base de las políticas establecidas por la institución.
- c) Debe habilitarse una cuenta auxiliar para cada cliente, funcionario o empleado.
- d) Deben realizarse arqueos periódicos de los documentos para conciliarlos con los libros contables.
- e) Las autorizaciones para descargo de cuentas malas deben ser aprobadas en atención a las normas contables y leyes que existan para tales fines.
- f) Se deben depurar los pedidos de cada cliente antes de despachar las mercancías o prestar los servicios.
- g) Emitirse mensualmente un análisis de los saldos de cuentas por cobrar.
- h) Emitir mensualmente un estado de cuenta a cada cliente.
- i) Emitir un recibo provisional de cobro prenumerado.
- j) El encargado de cuentas por cobrar no podrá tener control sobre los asientos contables de los cobros realizados.
- k) Asignar códigos a los cobradores a domicilio.
- l) Dividir por zonas a los cobradores y los clientes para mejor control.
- m) Asignar un código a cada cuenta por cobrar.
- n) Los recibos de cobro deben estar prenumerados de Imprenta.
- o) Determinar políticas para una gestión de cobros eficiente.
- p) Enviar a cada departamento correspondiente copias de las cuentas por cobrar para las futuras operaciones y registro de las mismas.
- q) Mantener control de aquellas cuentas que se estimen de dudoso cobro aunque ya estén fuera del sistema.
- r) Emitir informe para la gerencia de las cuentas recuperadas.

- s) Realizar un presupuesto mensual estimado de los cobros a realizar.
- t) Realizar llamadas de recordatorio de pagos a los clientes.

3.3.4 Procedimientos de control interno de: entrada de datos, el procesamiento de información y la emisión de resultados

Son de gran ayuda por la confiabilidad que brindan en el procesamiento de información, permiten verificar que el procedimiento de entrada-proceso-salida se lleve a cabo correctamente.

- a) Verificar la existencia y funcionamiento de los procedimientos de la captura de datos.
- b) Comprobar que todos los datos sean debidamente procesados.
- c) Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos.
- d) Comprobar la oportunidad, confiabilidad y veracidad en la emisión de los resultados del procedimiento de información.

a) Verificar la existencia y funcionamiento de los procedimientos de la captura de datos electrónicamente:

El trabajo de informática se inicia con la entrada de los datos que serán procesados en el sistema de información; por esta razón, es de vital importancia adoptar este subelemento del control interno, a fin de asegurar que la entrada de los datos será acorde con las necesidades de captura del propio sistema. Si se considera que el objetivo final de un sistema de computación es el procesamiento de los datos capturados, la siguiente frase cobra vigencia para el cabal entendimiento de este subelemento: si captura basura en el sistema de cómputo, como resultado de su procedimiento se obtiene basura. Al analizar lo anterior, es evidente que se necesita establecer un adecuado control en la entrada de los datos que han de ser procesados en cualquier sistema computacional, ya que de esto depende que se obtengan buenos resultados de ese proceso; además, con la adopción del control interno

se busca que los resultados del procesamiento de los datos sean los esperados por el usuario, a fin de utilizarlos de manera oportuna, confiable y adecuada.

Para lograr la eficiencia y la eficacia que se pretenden al establecer este elemento en la captura de datos, es necesario tener bien establecidos aquellos métodos, procedimientos y actividades que regularán la entrada de los datos del sistema, así como las normas políticas y lineamientos que ayudarán a capturar mejores datos. Con esto se garantiza que el procedimiento de información y la emisión de resultados sean adecuados. Con la implementación de este subelemento también se pretende dar validez y veracidad a los datos que entran al sistema para lo cual se establecerán los procedimientos, métodos, pruebas y verificaciones que se deben realizar durante los procesos de captura por ejemplo: el establecimiento de cifras de control, el cotejo de datos, la captura doble de la información, los chequeos aleatorios de datos y muchos otros exámenes que garanticen la veracidad y confiabilidad de los datos introducidos al sistema. Sin embargo, no basta con verificar la entrada correcta de los datos capturados, también es necesario comprobar que éstos sean introducidos con la oportunidad que demanda el sistema; esto se verifica con los siguientes procedimientos:

- ✓ El establecimiento y cumplimiento de los procedimientos adoptados para satisfacer las necesidades de captura de información de la empresa.
- ✓ La adopción de actividades específicas que ayuden a la rápida captura de los datos.
- ✓ El seguimiento de los métodos y técnicas uniformes que garanticen que la entrada al sistema se realice siguiendo procedimientos.

En consecuencia, con la aplicación de los procedimientos anteriores se puede garantizar la uniformidad en la entrada de datos, siempre que se

utilicen los mismos métodos, técnicas y procesos en tiempos similares, garantizando con ello la oportunidad y utilidad de la información.

Para el buen funcionamiento de este subelemento del control interno, se tienen que contemplar las estructuras que deben tener las bases de los datos a fin de prevenir posibles problemas de captura, como pueden ser las redundancias, los desajustes de datos, las repeticiones de información o cualquier otra contrariedad que llegue a efectuar la introducción de datos al sistema. También se debe contemplar la seguridad y la protección en la captura de la información, aspectos que serán tratados en otro subelemento del control interno.

b) Comprobar que todos los datos sean debidamente procesados

Además de verificar que los datos sean capturados y procesados de manera oportuna, confiable y eficiente, igual que en la emisión de los resultados. También es indispensable que con el control interno informático se tenga la confianza de que todos los datos ingresados al sistema sean procesados de igual manera sin que sufran ninguna alteración, ya sea accidental, involuntario o dolorosa, durante su procedimiento. Cumpliendo con esto se garantiza la uniformidad de los resultados y consecuentemente, se obtiene una mejor exploración de los mismos. Se debe remarcar que el procesamiento de datos se debe realizar de la misma manera en todos los casos, sin admitir ninguna variación en lo más mínimo; esto casi se cumple, ya que antes de liberar un sistema previamente se comprueban los procedimientos de información, primero mediante pruebas con datos falsos, similares a los que se utilizarán en el sistema y posteriormente mediante pruebas con datos reales; una vez aprobado su funcionamiento, se libera el proyecto con la plena confianza de que su procedimiento interno será siempre igual. Esto por sí solo justifica la adopción de este subelemento del control interno; sin embargo, además de lo antes señalado, también es

necesario establecer métodos, procedimientos y lineamientos en el área de sistema para evitar la existencia de algún tipo de información implementada en la empresa.

c) Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos

Para implementar este subelemento del control interno, es necesario entender que no basta con verificar la confiabilidad de la captura de los datos, sino que también se debe evaluar la veracidad de los datos que se introducen al sistema. Además, es imperioso comprobar la exactitud y suficiencia en el procesamiento de dichos datos, para lo cual es necesario establecer los procedimientos adecuados que ayuden a satisfacer los requerimientos de captura y procesamiento de información en el área de sistemas.

Sin embargo, para el buen funcionamiento de este subelemento, también se deben adoptar acciones concretas que ayuden a capturar y a procesar los datos de manera eficiente; para ello se tienen que establecer métodos, técnicas y procedimientos que sean aplicados de manera uniforme en todas las etapas que intervienen en el procesamiento de información; con esto se pueden garantizar mejores resultados en la verificación de la uniformidad que requiere este subelemento del control interno informático.

Se debe señalar que lo que se busca con este subelemento del control interno es la implementación de los métodos, técnicas y procedimientos que ayuden a uniformar las actividades requeridas en el área de sistematización para la captura de datos, el procesamiento de información y la emisión de informes.

d) Comprobar la oportunidad, confiabilidad y veracidad en la emisión de los resultados del procedimiento de información:

Si partimos de que el objetivo básico de un centro de cómputo es proporcionar los servicios de procesamiento de datos que requiere la empresa para satisfacer sus necesidades de información, entonces se entiende que uno de los aspectos fundamentales de un centro de cómputo es proporcionar la información que requieren las demás áreas de la empresa, con lo cual construye a satisfacer sus necesidades de procesamiento de datos.

Sin embargo, esa información debe ser adecuada a los requerimientos de la empresa para ofrecer sólo la información requerida, sin dar ni más ni menos datos que los necesarios. A esto se llama proporcionar la información suficiente.

Precisamente esto es lo que se busca satisfacer con la suficiencia de información; para lograrlo, es necesario que el área de sistemas tenga conocimiento de los requerimientos reales y específicos de información del usuario; esto se logra mediante un análisis adecuado de sus necesidades y con diseño correcto de los sistemas que proporcionarán esa información. Evidentemente, dicha suficiencia sólo se logrará mediante un buen análisis y diseño de sistemas.

De lo anterior es fácil comprender que el establecimiento de este subelemento del control interno informático es una necesidad básica en las áreas de sistematización, ya que con este control se verifica que la información proporcionada al usuario sea, ni más ni menos, la necesaria para satisfacer sus requerimientos fundamentales para la realización de sus actividades cotidianas.

3.3.5 Procedimientos de control interno para la seguridad del área de sistemas

Seguridad de los recursos informáticos, del personal, de la información, de sus programas y otros, lo cual se puede lograr a través de medidas preventivas o correctivas, o mediante el diseño de programas de prevención de contingencias para la disminución de riesgos.

- a) Control sobre la seguridad física del área de sistemas.
- b) Control sobre la seguridad lógica de los sistemas.
- c) Control sobre la seguridad de las bases de datos.

a) Control sobre la seguridad física del área de sistemas

Con este tipo de controles se busca salvaguardar los activos tangibles de la empresa en este caso específico, es la sistematización para la protección y custodia de los equipos de cómputo, periféricos, mobiliario y equipo asignado a esa área, así como la protección y seguridad del personal, de los usuarios y el demás personal involucrado en el centro de cómputo.

Es de suma importancia destacar que el establecimiento de este subelemento del control interno informático ayudará enormemente a salvaguardar los activos informáticos tangibles del área de sistemas, con los cuales se realizan sus actividades y el cumplimiento de sus tareas.

Para el mejor entendimiento de la adopción de este subelemento, y aunque existen muchos controles para la prevención de contingencias y salvaguardar de estos recursos informáticos, a continuación se proponen algunos controles básicos que deberán ser adoptados en las áreas de sistematización para la protección de sus recursos; sin embargo, las empresas deberán determinar estos controles de acuerdo con sus características, necesidades y condiciones específicas de procesamiento de información.

- ✓ Inventario del hardware, mobiliario y equipo
- ✓ Procedimiento para resguardo del equipo de cómputo
- ✓ Procedimiento de bitácoras de mantenimientos y correcciones
- ✓ Procedimiento de controles de acceso del personal al área de sistemas
- ✓ Procedimiento de control del mantenimiento a instalaciones y construcciones
- ✓ Procedimiento de seguros y fianzas para el personal, equipos y sistemas
- ✓ Procedimiento de contratos de actualización, asesoría y mantenimiento del hardware

b) Control sobre la seguridad lógica de los sistemas

Así como es necesario establecer controles para salvaguardar los bienes físicos del sistema computacional en la empresa, también es necesario establecer controles y medidas preventivas y correctivas para salvaguardar sus bienes lógicos. Con ello se pretende un buen uso del software, de los programas, de los sistemas operativos, del procesamiento de información, de los accesos al sistema, de la información, otros.

Cabe aclarar que estos controles se deben establecer de acuerdo con el tipo de sistemas de la empresa, al tamaño y configuración de su equipo, a la forma de procesamiento de su información y de sus características concretas y procedimientos de operación, así como de acuerdo con los lenguajes de programación, paquetería, programas y aplicaciones concretas que se realizan con el sistema computacional.

A continuación se proponen algunos controles que se deben considerar en la seguridad lógica, los cuales, al igual en las secciones anteriores, se tienen que establecer de acuerdo con las características y necesidades de procesamiento de la empresa.

- ✓ Control para el acceso al sistema, a los programas y a la información
- ✓ Procedimientos de establecimiento de niveles de acceso
- ✓ Procedimientos de dígitos verificadores y cifras de control
- ✓ Procedimientos de palabras clave de accesos

c) Control sobre la seguridad de las bases de datos

El activo más importante de cualquier empresa es la información que se captura, que se procesa y que se emite en las bases de datos de los sistemas; por lo tanto, es el bien que más se debe proteger.

El control interno informático ayuda a proteger las bases de datos de la empresa, por medio de controles especiales y medidas preventivas y correctivas. Con las restricciones de acceso al sistema se puede evitar posibles alteraciones, uso fraudulento, piratería, destrucción y sabotaje de la información de la empresa. Estos controles pueden ser establecidos por el área administrativa para vigilar al acceso de los usuarios al sistema, así como para proteger la información a través de respaldos periódicos y recuperación de datos en caso de pérdidas, deterioros y de cualquier mal uso que se haga de ellos. Los siguientes son algunos 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.
- ✓ Planes y programas para prevenir contingencias y recuperar información.
- ✓ Control de accesos a la bases de datos.
- ✓ Rutinas de monitoreo y evaluación de operaciones relacionados con base de datos.

CAPÍTULO IV
EL PAPEL DEL CONTADOR PÚBLICO Y AUDITOR, COMO AUDITOR
INTERNO EN LA ELABORACIÓN DE PROCEDIMIENTOS DE CONTROL
INTERNO EN PREVENCIÓN DE FRAUDES INFORMÁTICOS EN EL ÁREA DE
CUENTAS POR COBRAR DE UNA EMPRESA DE TRANSPORTE TERRESTRE
(CASO PRÁCTICO)

4.1 ANTECEDENTES DE LA EMPRESA

Es una empresa fundada en el año 2001 en la ciudad de Guatemala, en constante evolución, se dedica a prestar servicio de transporte terrestre nacional desde su fundación se ha caracterizado por contar con tecnología moderna para el registro de sus operaciones y procesos administrativos.

Esta empresa ofrece una amplia gama de servicios como transporte de bienes y cosas, maquinaria pesada y liviana. Cuenta con el transporte idóneo para prestar un servicio de calidad y de satisfacción para el cliente.

➤ **Transporte terrestre nacional**

- a) Transporte de cargas interdepartamentales. (Escuintla, Izabal, San Marcos, Chiquimula, etc.)
- b) Transporte de carga en camiones puerta a puerta en toda Guatemala.
- c) Transporte terrestre internacional.

➤ **Los equipos que tienen para prestar los diferentes servicios son:**

- a) Equipos especializados en transporte de mobiliario y menaje de casa.
- b) Equipos para cargas refrigeradas.
- c) Equipos para cargas sobredimensionadas.
- d) Equipos para cargas consideradas peligrosas.

➤ **Personal**

Roxaluna, S.A., es una empresa que cuenta actualmente con 52 empleados; administración 12 personas y operaciones 40. Sucursales no tiene, su centro de operación es en la ciudad de Guatemala por el tipo de relaciones comerciales aún no es necesario abrir otras sedes ya que la mayoría de negocios se cierran en la capital. Sus jefaturas están divididas de la siguiente forma:

- ✓ Junta General de Accionistas
- ✓ Junta Directiva
- ✓ Presidencia
- ✓ Vicepresidencia
- ✓ Gerencia General
- ✓ Recursos Humanos
- ✓ Gerencia Financiera
- ✓ Gerencia Operaciones
- ✓ Gerencia Ventas

➤ **Unidades para el servicio**

Para el desarrollo de sus actividades mercantiles cuentan con las siguientes unidades:

- ✓ 3 Cabezales para carga pesada incluye su plataforma
- ✓ 7 Camiones de 10 toneladas
- ✓ 2 Camiones de 3.5 toneladas
- ✓ 2 Microbuses

➤ **Estructura de las cuentas por cobrar dentro del Estado de Situación Financiera**

Dada la importancia de las ventas al crédito en relación a las cifras del Estado Situación Financiera, se analizó la cartera el día 10 de abril de 2014, del período del 01 de enero al 31 de diciembre de 2013, el monto de la cartera representada el 29% del total del activo.

Tabla 1
Roxaluna, S.A.
Estado de Situación Financiera del 01 de Enero al 31 de Diciembre 2013
Revisión Analítica

(Expresada en quetzales)

ACTIVO CORRIENTE		2013	%	PASIVO CORRIENTE		2013	%
Caja y Bancos		1,225,000.00	12	Cuentas por Pagar		355,000.00	3
Cuentas por Cobrar		3,000,000.00	29	Proveedores		325,000.00	3
Inversiones		1,400,000.00	14	Provisión para cuentas incobrables		75,000.00	1
Inventarios		1,500,000.00	15	Sub-total		755,000.00	
ACTIVO NO CORRIENTE				PASIVO NO CORRIENTE			
Propiedad Planta y Equipo		1,715,000.00	17	Documentos por Pagar Largo Plazo		500,000.00	5
Gastos Pagados por Anticipados		550,000.00	5	Préstamos a Largo Plazo		800,000.00	8
Otros activos		865,000.00	8				
Sub-total		3,130,000.00		Sub-total		1,300,000.00	
PATRIMONIO Y CAPITAL							
Sub-total		7,125,000.00		Patrimonio		8,200,000.00	80
TOTAL ACTIVO				TOTAL PASIVO Y PATRIMONIO			
		10,255,000.00	100			10,255,000.00	100

Nota. El estado de resultados de la empresa Roxaluna, S.A. muestra la situación financiera de la empresa al 31 de diciembre del 2013.

4.2 CONSTITUCIÓN Y ORGANIZACIÓN

La empresa se constituyó el 10 de enero del año 2001, con el objetivo principal de prestar servicios de transporte terrestre, se hicieron los trámites correspondientes ante el Registro Mercantil, el Instituto Guatemalteco de Seguridad Social y la Superintendencia de Administración Tributaria.

a) Registro Mercantil

Debe registrarse el tipo de empresa que se desea inscribir, (comerciante o empresa individual o algún tipo de sociedad mercantil). La empresa una vez registrada recibirá su Patente de Comercio, que es el documento que acredita la inscripción de la empresa ante el Registro Mercantil.

b) Instituto Guatemalteco de Seguridad Social

El IGSS fue creado por el Decreto No. 295 del Congreso de la República de Guatemala actualmente se encuentra anexada al Ministerio de Trabajo y Previsión Social, sin embargo esto no impide su autonomía. La empresa debe estar registrada como patrono ante el Instituto Guatemalteco de Seguridad Social (IGSS), para efectuar las retenciones y pago de la cuota laboral, así como de las cuotas patronales.

c) Superintendencia de Administración Tributaria, SAT

Entidad estatal descentralizada, que ejerce con exclusividad las funciones de administración tributaria contenidas en la legislación. Su misión es recaudar los recursos (impuestos) provenientes de los actos gravados. Toda empresa debe registrar sus operaciones ante la Superintendencia de Administración Tributaria (SAT), quién autorizará los libros contables, facturas a utilizar, cajas o máquinas registradoras.

➤ **Impuesto al valor agregado (IVA)**

Esta ley, contenida en el Decreto 27-92, establece un Impuesto al Valor Agregado sobre los actos y contratos gravados por ésta, cuya administración, control, recaudación y fiscalización corresponde a la Superintendencia de Administración Tributaria (SAT). Dichos actos y contratos afectos, los encontramos de forma específica en el hecho generador del artículo tres (3) de la misma.

Las empresas afectas a las disposiciones de esta ley, pagarán el impuesto de una tarifa única del doce por ciento (12%) sobre la base imponible, porcentaje que deberá estar incluida en el precio de venta de los bienes o el valor de los servicios.

La suma neta que el contribuyente debe enterar al fisco mensualmente, es la diferencia entre el total de débitos y el total de créditos fiscales generados. (Art. 19 ley)

➤ **Impuesto sobre la renta (ISR)**

Toda empresa esta afecta a las disposiciones legales contenidas en el Decreto 10-2012 LEY DE ACTUALIZACIÓN TRIBUTARIA LIBRO I. Quedan afectas al impuesto todas las rentas y ganancias de capital obtenidas en el territorio nacional. El impuesto se genera cada vez que se producen rentas gravadas y se determina de conformidad con lo que establece dicha ley. Son contribuyentes del impuesto, las personas individuales y jurídicas, domiciliadas o no en el país, que obtengan rentas en el país independientemente de su nacionalidad o residencia y por lo tanto están obligadas al pago del impuesto cuando se verifique el hecho generador del mismo.

➤ **Impuesto de solidaridad, ISO**

Las disposiciones legales de esta ley, Decreto número 73-2008, establece un hecho generador por la realización de actividades mercantiles o agropecuarias en el territorio nacional, para las personas, entes o patrimonios a que se refiere el 12 artículo uno de la ley y que los ingresos brutos sean superiores al 4%. Dicha ley establece algunas exenciones para algunas entidades tal como se establece en el artículo cuatro (4) de la misma.

El tipo impositivo que establece, es la del 1%, que será multiplicado por la base imponible establecida por las dos opciones que establece el artículo 7, que no es más que; la cuarta parte de monto del activo neto o la cuarta parte de los ingresos brutos.

➤ **Impuesto de timbres fiscales y del papel sellado especial para protocolos**

Esta ley, está contenida en el Decreto 37-92 y recae sobre los documentos que contienen actos y contratos que se expresan en la ley según el artículo dos (2) de la misma, ya que los sujetos pasivos son; quienes emitan, suscriban u otorguen documentos que contengan actos o contratos objeto de tal emisión, suscripción u otorgamiento. La tarifa del impuesto es del 3% aplicado al valor de los actos y contratos afectos, la cual no podrá ser inferior al que conste en los registros públicos, matrículas, catastro o en los listados oficiales.

➤ **Código tributario**

Las normas del Código Tributario Decreto 6-91, son aplicables a las infracciones y sanciones, estrictamente en materia tributaria, salvo lo que dispongan las normas especiales que establezcan las leyes que regulan cada tributo (Art. 67), Es así, como las empresa deberán tener sumo cuidado en no cometer ningún tipo de acción u omisión que implique violación de normas tributarias de índole sustancial o formal, ya que será sancionada por la Administración Tributaria (SAT), en tanto no constituya delito o falta sancionados conforme a la legislación penal. (Art. 69)

➤ **Ley de productos financieros (IPF)**

Según esta Ley Decreto 26-95 del Congreso de la República, es que grava los ingresos por intereses de cualquier naturaleza generados en el momento del pago o acreditamiento de intereses. Están obligadas las personas individuales o jurídicas domiciliadas en el país, que obtengan ingresos por concepto de intereses con excepción de las personas sujetas a la fiscalización de la Superintendencia de Bancos (SB). La base imponible de este impuesto lo constituye la totalidad de los ingresos por concepto de intereses multiplicado por el tipo impositivo del 10%.

Código de trabajo

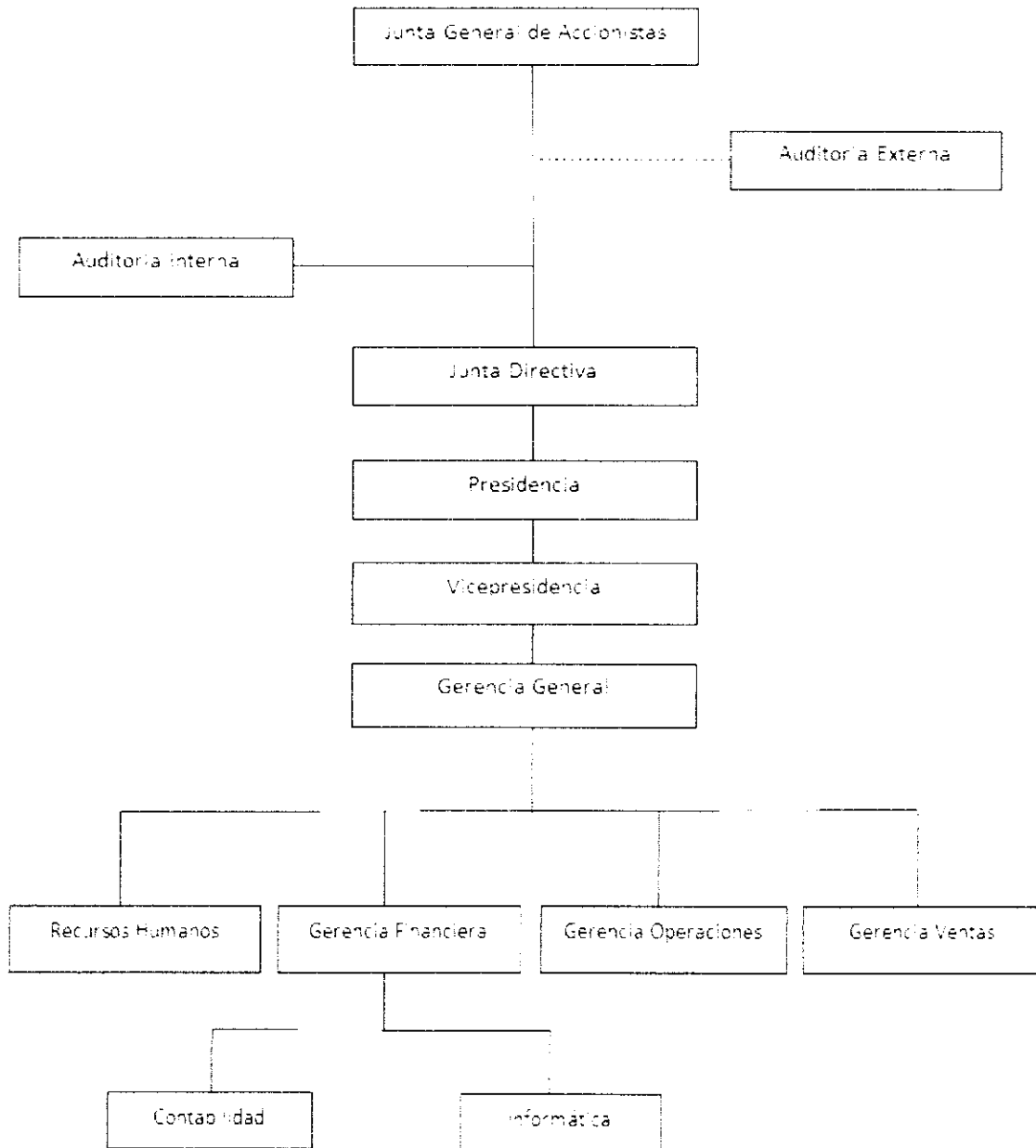
Según Decreto 1441, este código establece los derechos y obligaciones de patronos y trabajadores, con ocasión del trabajo y crea instituciones para resolver sus conflictos, tal como lo señala el artículo uno (1) de la ley. Dicha ley son adoptadas por todas las empresas en Guatemala, ya que norma la relación patrono-trabajador, mediante un contrato individual de trabajo.

También deberá regirse por otras leyes, tales como:

- Código Penal (Decreto 17-73 y sus reformas)
- Disposiciones Legales para el Fortalecimiento de la Administración (Decreto 20-2006).
- Ley Orgánica del Instituto Guatemalteco de Seguridad Social (Decreto 295)
- Código aduanero uniforme centroamericano (resolución No. 223 2008)

4.3 ORGANIGRAMA

Figura 2
Roxaluna, S.A.



Fuente: departamento de recursos humanos de la compañía objeto de estudio.

4.4 GENERALIDADES

El sistema operativo que trabaja la empresa es SQL y el proceso contable es manejado a través de un sistema informático desarrollado en una base de datos VISUALBASIC, el cual a criterio de la administración es confiable.

El Gerente General manifiesta aunque no tienen problemas serios con el sistema de contabilidad, él reconoce como avanza la tecnología de la informática y le preocupa de que no tener los controles internos informáticos necesarios para hacerle frente a este nuevo reto, adicionalmente, sabe que así como se abren nuevas oportunidades de negocio, conoce riesgos que le acompañan. Por tal razón, desea actualizarse y verificar que el sistema de contabilidad en el área de cuentas por cobrar de la empresa Roxaluna, S.A., llene los requisitos que le permitan estar preparado para esta nueva era de los sistemas informáticos.

Para lo antes mencionado nos presenta cuál es su situación actual y como está compuesto su sistema contable.

El módulo de clientes está compuesto por 4 tablas de datos (Bases de Datos)

- 1- Datos de clientes
 - 2- Datos de facturas (información de la factura.)
 - 3- Datos de registros contables
 - 4- Datos de registro de auxiliares de cuentas por cobrar.
- El sistema contable fue instalado hace 2 años, Las modificaciones al sistema se pueden realizar siempre y cuando no afecten la estructura del mismo.
 - Todas las operaciones son realizadas en tiempo reales
 - El programa fuente está instalado en una computadora (Servidor), la empresa que lo instaló aún le presta servicio de soporte.

El programa es trabajado a través de terminales que están conectados en una red doméstica.

El servidor está en el departamento de cómputo.

El proceso de emisión de facturas hasta su cancelación está integrado por tres procesos:

- 1- Orden de facturación
- 2- Emisión de factura
- 3- Cobro y depósito de factura

➤ **Orden de facturación**

Es ejecutada por el departamento ventas, a través de una cotización ya autorizada por el cliente. Después de que se ejecuta el trabajo y se finaliza se procede a emitir su respectiva orden de facturación la cual es impresa y trasladada al departamento de contabilidad.

➤ **Emisión de factura**

El Departamento de contabilidad recibe la orden de facturación y la ejecuta en 4 pasos:

- 1- Creación del Cliente (si es un cliente nuevo)
- 2- Elaboración de la factura.
- 3- Ingreso de partida contable así como el auxiliar de clientes que se registra automáticamente.
- 4- Impresión de la factura.

➤ **Cobro y depósito de factura.**

Al recibir el cheque o el pago en efectivo del cliente se envía con su respectiva boleta bancaria a uno de los bancos del sistema.

➤ **Operación contable**

Al tener el departamento de contabilidad su boleta respectiva sellada por el banco, se opera en los libros de bancos, así como contablemente y se cancela su auxiliar respectivo.

Cuando el pago es en efectivo se opera igual que los cheques, el efectivo se envía a los bancos del sistema.

Cuando se realizan abonos parciales, los mismo son operados sólo a nivel contable, no se opera el abono respectivo a los auxiliares.

Cuando el banco nos rechaza un cheque por no tener fondos, se solicita un nuevo cheque al cliente y se realiza un redepositó. No se realiza ninguna operación contable.

➤ **Archivo**

Después que se ejecutan los 2 pasos anteriores se procede a archivar el depósito con su respectiva papelería de soporte.

➤ **Reportes**

Mensualmente se emite el reporte de antigüedad de clientes, el cual se verifica que sea igual al saldo de contabilidad.

4.5 TRABAJO A DESARROLLAR

A raíz de la preocupación de la administración de la empresa en prevenir fraudes, es que se ha visto en la necesidad de utilizar los servicios del Contador Público y Auditor Interno de la empresa, para que le presente procedimientos necesarios que le permitan mejorar su control interno informático en el área de cuentas por cobrar.

El trabajo a desarrollar será la elaboración de procedimiento de prevención de fraudes informáticos en la cuenta por cobrar para llegar a los resultados antes mencionados se deberá tomar como base Las Normas Internacionales de Auditoria y Normas Internacionales para el Ejercicio Profesional de la Auditoria Interna.

4.6 PAPELES DE TRABAJO

ROXALUNA, S.A.
INDICE DE PAPELES DE TRABAJO
31 de diciembre del 2013

Referencia	Papeles de Trabajo	Página
NL	Nombramiento	82
MP	Memorándum de planificación	83
PTI	Programa de trabajo	85
CI	Cuestionario de control interno cuentas por cobrar	86
CI	Cuestionario de control interno área del sistema	87
CI	Matriz de riesgos área de cuentas por cobrar	89
CI	Matriz de riesgos área del sistema	90
CI	Matriz de evaluación del riesgo inherente	91

ROXALUNA, S.A.
AUDITORIA INTERNA

Nombramiento:

Guatemala 01 de abril de 2014

Señor (es): Lic. Adrián Pineda –Auditor Interno

Por este medio se le (s) comunica que ha (n) sido designado para ejecutar lo siguiente:

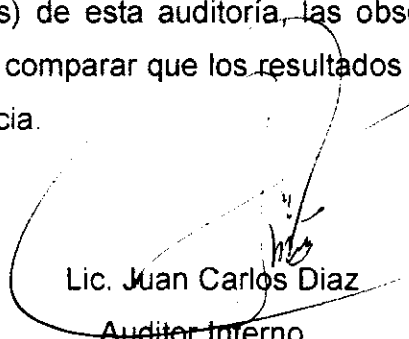
Trabajo: auditoría de procedimientos convenidos para la prevención de fraudes informáticos en el rubro de cuentas por cobrar.

Referido al: 31 de diciembre de 2013

Inicio de la auditoria:	01/04/2014, a las 08:00 horas.
Terminación de la auditoria:	10/04/2014, a las 17:00 horas.
Discusión del informe preliminar:	14/04/2014, a las 08:00 horas.
Entrega del informe final:	17/04/2014, a las 17:00 horas

Se le (s) recomienda: a) comunicar inmediatamente al suscrito las anomalías que por su carácter demanden una acción urgente; b) elaborar las cédulas donde conste (n) el (los) resultado (s) de esta auditoría, las observaciones de valor u orden que sean necesarias; c) comparar que los resultados obtenidos sean reales e informar de cualquier diferencia.

Atentamente,



Lic. Juan Carlos Díaz
Auditor Interno

ROXALUNA, S.A.
CUENTAS POR COBRAR AREA INFORMÁTICA
MEMORANDO DE PLANIFICACIÓN
AL 31-12-2013

I. Programación de actividades

Inicio de trabajo de campo	01-04-14
Terminación de trabajo de campo	10-04-14
Entrega de Informe	17-04-14

II. Objetivo de la evaluación

Evaluar el control interno informático en las cuentas por cobrar. Dar a conocer sus deficiencias de control interno informático detectadas. Presentación de procedimientos para prevenir las debilidades encontradas.

III. Generalidades y operaciones

La empresa se dedica a la prestación de servicios de transporte de bienes muebles y cosas de un lugar a otro. Sus ingresos dependen de los servicios prestados.

IV. Controles gerenciales

La estructura de control interno informático implementado en la empresa, necesita ser evaluada para corregir las deficiencias del mismo. Los miembros del Consejo de Administración, son quienes finalmente toman las decisiones trascendentales.

V. Personal clave

Gerente General
Gerente Financiero
Contador General

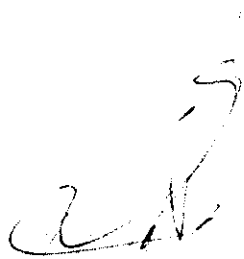
VI. Evaluación de control interno informático

El sistema de control interno informático no es muy voluminoso, sin embargo es necesario familiarizarse respecto a las funciones de las cuentas por cobrar.

VII. Trabajo a realizar

Entrevistar al Contador General, a efecto de conocer el procedimiento completo y posteriormente aplicar cuestionario de evaluación de control interno, técnicas que permitirán familiarizarse con los procedimientos del área de cuentas por cobrar.

Examinar la documentación de soporte y demás procedimientos establecidos por la administración. Para el efecto se prepararán los papeles de trabajo, que permitirán respaldar nuestro informe con los procedimientos respectivos.



Lic. Adrián Pineda
Contador Público y Auditor
Colegiado CPA-9110728
Colegio de Contadores Públicos y Auditores

ROXALUNA, S.A.,
 CUENTAS POR COBRAR
 PROGRAMA DE TRABAJO
 AL 31 DE DICIEMBRE 2013

PTI	FIRMA	FECHA
Realizó	AP	01/04/2014
Revisó	JCD	08/04/2014

No.	Procedimiento	Auditor	Fecha	Ref.
1	Evaluar el control interno en el área de cuentas cobrar por medio de cuestionarios dirigidos al contador general	AP	02/04/2014	C/I
2	Revisar los procedimientos de registro de los ingresos, operación y salida de la información del sistema por medio de cuestionarios dirigidos al contador general	AP	08/04/2014	C/I
3	Evaluar el control interno informático por medio de cuestionarios dirigidos al contador general.	AP	04/04/2014	C/I
4	Realizar matriz de riesgos de cuentas por cobrar del sistema y evaluación del riesgo inherente.	AP	08/04/2014	C/I

ROXALUNA, S.A.

CUESTIONARIO DE CONTROL INTERNO AREA DE CUENTAS POR COBRAR
31 DE DICIEMBRE 2013

PT: C/I	Firma	Fecha
Realizó	AP	02/04/2014
Revisó	JCD	08/04/2014

No.	CONTESTE		
	SI	NO	OBSERVACIONES
CRÉDITOS:			
1.-	X		¿Aprueba todas las notas de crédito un funcionario responsable quien no es el que opera ventas, cobros ni auxiliares de clientes? Se revisaron las notas de crédito respectiva
2.-	X		¿Aprueba un funcionario responsable las cancelaciones de cuentas de clientes dudoso? Se revisaron y si estan aprobadas
3.-	X		¿Se comprueba la secuencia numérica de las facturas? Se reviso la numeracion
4.-	X		¿Se comprueba la secuencia numérica de las notas de crédito? Se reviso la numeracion
REGISTRO Y COBROS:			
5.-	X		¿Proporciona un empleado independiente del encargado de las cuentas de clientes, los totales por cobros y por notas de crédito que deben registrarse en el libro mayor? Se le solicito y se verifico que si era un empleado diferente el que las proporciono
6.-		X	¿Se registran los cheques rechazados de los clientes?
7.-		X	¿Existe un procedimiento formal para el manejo de los redepositos?
8.-		X	¿Se registran los abonos parciales en el mayor y en el auxiliar de clientes.?
9.-	X		¿Los registros de clientes del mayor y los auxiliares estan cuadrados? Se verifico cuenta contable y auxiliar de clientes
10.-	X		¿La conciliación de la cuenta de clientes así como el auxiliar son revisados por otra persona que no es el responsable del manejo de los clientes.? Se solicito la informacion para verificar
11.-		X	¿Se cancelan todas las facturas con recibos de caja?
12.-		X	¿Existe un procedimiento para los pagos recibidos en efectivo?
13.-	X		¿Revisa un funcionario responsable los saldos de clientes para asegurarse de crédito autorizados, de que no esten atrasados? Se verifico antigüedad de saldos clientes
14.-		X	¿ Se envían mensualmente estados de cuenta a los clientes?
15.-	X		¿Custodia los documentos y facturas por cobrar un empleado que no sea el: a) Cajero? b) Encargado de auxiliar de clientes? Se solicitaron lo archivos para confirmacion
CLIENTES			
16.-	X		¿Se requiere que las aceptaciones y renovaciones de créditos así como la solicitud de notas de crédito y anulaciones de facturas sean aprobadas por el gerente de crédito u otro funcionario responsable? Se revisaron anulacion y si estan firmadas
17.-	X		¿Se lleva auxiliar de las cuentas de clientes? Se solicitaron y revisaron fisicamente
18.-		NA	¿Se registran las facturas de clientes descortados en cuenta separada del libro mayor?
19.-	X		¿Se tiene un registro general de la informacion del cliente ? Se confirmo el archivo general de clientes
20.-	X		¿Se concilian la cuenta de clientes según auxiliares o reportes emitidos que no sean contables.? Se verificaron y se confirmo lo indicado
COBRADORES			
21.-		X	¿Existe la politica de utilizar cobradores para efectuar cobros?
22.-	X		¿Están ajenos los cobradores a las funciones de venta y aprobación de crédito? a) Se basa su remuneración en montos cobrados b) Existe un procedimiento para los pagos que reciben en efectivo que sean entregados de inmediato a la persona responsable de los depósitos Si se reviso y no tienen ninguna ingerencia de la aprobacion de creditos Se observo los cuadros de caja chica de los cobradores y el procedimiento

ROXALUNA, S.A.

CUESTIONARIO DE CONTROL INTERNO AREA DE SISTEMAS
31 DE DICIEMBRE 2013

PT: C/I	Firma	Fecha
Realizó	AP	02/04/2014
Revisó	JCD	04/04/2014

No.	CONTESTE	CONTESTE		OBSERVACIONES
		SI	NO	
CAPTACION E INGRESOS				
1.-	El 75% de información de clientes es manejada a través del sistema	X		Se verifico la operación y manejo de este modulo
2.-	¿Se verifica la información recibida para su captura?	X		Se verifico la operación y manejo de este modulo
3.-	¿Se revisan las cifras antes de enviarlas a captura?	X		Se verifico la operación y manejo de este modulo
4.-	¿Capturada la información puede modificarse despues de haberse ingresado?	X		Se verifico la operación y manejo de este modulo
5.-	¿Cuando la información ya esta grabada permite la modificación?	X		Se verifico la operación y manejo de este modulo
6.-	¿El programa verifica si los datos ingresados coinciden con el documento fuente?	X		Se verifico la operación y manejo de este modulo
7.-	¿Existe control para la captura de datos?		X	
8.-	¿Existe un registro de los documentos que entran a capturar?	X		Se verifico la operación y manejo de este modulo
9.-	¿Se hace un reporte diario, semanal o mensual de captura?	X	MENSUAL	Se confirmo con el reporte
10.-	¿Se hace un reporte diario, semanal o mensual de anomalías en datos de entrada?		X	
11.-	¿Se lleva un control de la operación en el sistema por persona?		X	
12.-	¿Quién revisa este control?		NA	
13.-	¿Existen instrucciones escritas para capturar de datos?		X	
OPERACIÓN				
14.-	¿Existen procedimientos formales para la operación del sistema de cómputo?	X		Se verifico la operación y manejo de este modulo
15.-	¿Están actualizados los procedimientos?	X		Se verifico la operación y manejo de este modulo
16.-	¿Existen procedimientos para la recuperación del sistema en caso de falla?	X		Se verifico la operación y manejo de este modulo
17.-	¿Se tienen procedimientos que indiquen al operador que hacer cuando un programa interrumpe su ejecución u otras dificultades en proceso?	X		Se verifico la operación y manejo de este modulo
18.-	¿Puede el operador modificar los datos de entrada?	X		Se verifico la operación y manejo de este modulo
19.-	¿Se prohíbe al programador la operación del sistema que programo?	X		Se verifico la operación y manejo de este modulo
20.-	¿Se prohíbe al operador modificar información de bases de datos del sistema?	X		Se verifico la operación y manejo de este modulo
21.-	¿Existe un control adecuado de los sistemas y programas que están en operación?	X		Se verifico la operación y manejo de este modulo
22.-	¿Se controlan los trabajos dentro del departamento de cómputo?	X		Se verifico la operación y manejo de este modulo
23.-	¿Se rota al personal de control de información con los operadores procurando un entrenamiento cruzado y evitando la manipulación fraudulenta de datos?		X	
24.-	¿Cuentan los operadores con una bitácora para mantener registros de cualquier evento y acción tomada por ellos?		X	
25.-	Verificar que exista un registro de funcionamiento que muestre el tiempo de paros y mantenimiento o instalaciones de software		X	
26.-	¿Existen procedimientos para evitar las instalaciones de programas no autorizados?		X	
27.-	¿Se restringe a los operadores el acceso a los diagramas de flujo, programas fuente, etc. fuera del departamento de cómputo?	X		Se verifico la operación y manejo de este modulo
28.-	¿Se controla estrictamente el acceso a la documentación de programas o de aplicaciones rutinarias?	X		Se verifico la operación y manejo de este modulo
29.-	¿Existen niveles de control que permita que el operador no pueda acceder a otras áreas de las cuales no tiene autorización?		X	
30.-	¿Todo programa ya instalado dentro del sistema es verificado para que cumpla con las ejecuciones solicitadas anteriormente?	X		Se verifico la operación y manejo de este modulo
31.-	Existe algún control en la operación que verifique que la información del sistema fue alterada?		X	
	¿Existe un lugar para archivar las bitácoras del sistema del equipo de cómputo?		X	
32.-	¿Se tiene inventario actualizado de los equipos y terminales con su localización?	X		Se verifico la operación y manejo de este modulo
33.-	¿Se controlan los procesos en línea?	X		Se verifico la operación y manejo de este modulo

ROXALUNA, S.A.

CUESTIONARIO DE CONTROL INTERNO AREA DE SISTEMAS
31 DE DICIEMBRE 2013

PT: C/I	Firma	Fecha
Realizó	AP	02/04/2014
Revisó	JCD	04/04/2014

No.		CONTESTE		OBSERVACIONES
		SI	NO	
34.-	¿Se tienen control sobre todos los equipos?	X		Se verifico la operación y manejo de este modulo
35.-	Se tiene control sobre las claves de acceso? (LA CLAVE FUNCIONA PARA ACCESO AL SISTEMA)		X	
	SALIDA			
36.-	¿Se tienen copias de los archivos en otros locales?		X	
37.-	¿Se verifica los documentos de salida con los documentos fuentes?	X		Se verifico la operación y manejo de este modulo
38.-	¿Los documentos de salida son manejados con confidencialidad?	X		Se verifico la operación y manejo de este modulo
39.-	¿Se posee una bitácora en los documentos de salida?		X	
40.-	¿Se tiene un responsable (usuario) de la información de los documentos de salida?		X	
41.-	¿Se pose un control para verificar la veracidad de los documentos de salida?	X		Se verifico la operación y manejo de este modulo
42.-	¿ Los documentos de salida están numerados correlativamente ?	X		Se verifico la operación y manejo de este modulo
43.-	¿Existe algún documento de salida que no este numerado?	X		Se verifico la operación y manejo de este modulo
44.-	¿Si la respuesta anterior es afirmativa escriba los nombres de los documentos de salida que no están numerados? LOS REPORTES Y LAS NOTAS DE CREDITO			
	ALMACENAMIENTO			
45.-	El local asignados para los archivos magnéticos tienen: Aire acondicionado	X		Se verifico las instalaciones físicas y el inventario
	Protección contra el fuego	X		Se verifico las instalaciones físicas y el inventario
46.-	¿Se verifican con frecuencia el inventario de los archivos magnéticos?	X		Se verifico las instalaciones físicas y el inventario
47.-	¿Los archivos con información confidencial cuenta con claves de acceso?		X	
48.-	¿Existe un control estricto de las copias de estos archivos?		X	
49.-	¿El almacenamiento de los archivos se realiza en un mueble con cerradura?	X		Se verifico las instalaciones físicas y el inventario
50.-	¿Se realizan auditorías periódicas a los medios de almacenamiento?		X	
51.-	¿El acceso a los dispositivos de almacenamiento, es restringido?	X		Se verifico las instalaciones físicas y el inventario
52.-	¿Existe un procedimiento para registrar los archivos que se prestan?	X		Se verifico las instalaciones físicas y el inventario
53.-	¿Se lleva control sobre los archivos prestados por la instalación?	X		Se verifico las instalaciones físicas y el inventario
54.-	¿Existe una persona responsable de la cinta maestra. ?	X		Se verifico las instalaciones físicas y el inventario
55.-	¿Se utiliza la política de conservación de archivos hijo-padre-abuelo?	X		Se verifico las instalaciones físicas y el inventario
	MANTENIMIENTO			
56.-	¿Existe un contrato de mantenimiento?	X		Se tuvieron a la vista los documentos de soporte
57.-	Existe un programa de mantenimiento preventivo de cómputo?	X		Se tuvieron a la vista los documentos de soporte
58.-	¿Se lleva a cabo tal programa?	X		Se tuvieron a la vista los documentos de soporte
59.-	¿Existen tiempos de respuesta estipulados en los contratos?	X		Se tuvieron a la vista los documentos de soporte
	EQUIPO DE COMPUTO			
60.-	¿Existe un inventario del equipo de computo?	X		Se tuvieron a la vista los documentos de soporte
61.-	¿Tienen las maquinas instaladas antivirus?	X		Se tuvieron a la vista los documentos de soporte
62.-	¿Están actualizados los antivirus?	X	X	Se tuvieron a la vista los documentos de soporte
63.-	¿Tienen acceso internet?	X		Se tuvieron a la vista los documentos de soporte

Persona entrevistada: Luis Pérez Puesto: Contador General Firma:

ROXALUNA, S.A.
MATRIZ DE RIESGO DE CUENTA POR COBRAR
 31 DE DICIEMBRE 2013

PT: C/I	Firma	Fecha
Realizó	AP	04/04/2014
Revisó	JCD	06/04/2014

PROCEDIMIENTO AREA DE CLIENTES	RIESGO DE FRAUDE
CRÉDITO	1
REGISTRO	3
CLIENTES	1
COBRO	1
	6

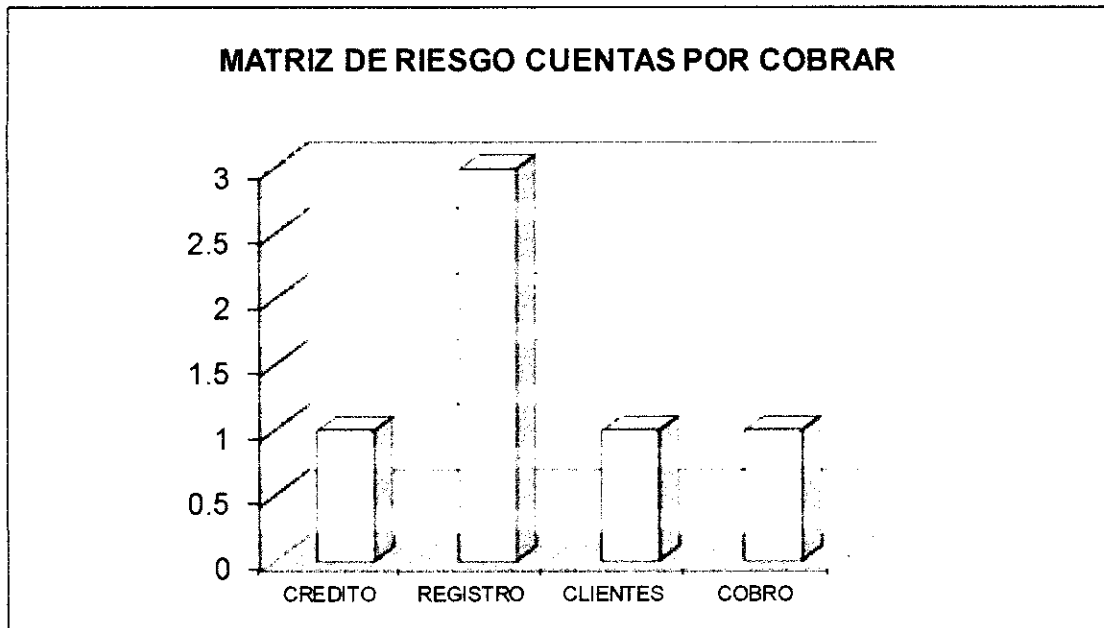
Riesgo de fraude

Nulo 0

Bajo 1

Medio 2

Alto 3



ROXALUNA, S.A.
 MATRIZ DE RIESGO DEL SISTEMA
 31 DE DICIEMBRE 2013

PT: C/I	Firma	Fecha
Realizó	AP	04/04/2014
Revisó	JCD	06/04/2014

	Suprimir u	Adicionar	Alterar	Duplicar	Riesgo
PROCEDIMIENTOS DE SISTEMA	Omitir Datos	Datos	Datos	Procesos	Fraude
CAPTACIÓN	1	1	1	2	20%
OPERACIÓN	0	0	0	2	8%
SALIDA	3	3	3	0	36%
ALMACENAMIENTO	3	3	3	0	36%
MANTENIMIENTO	0	0	0	0	0%
EQUIPO DE COMPUTO	0	0	0	0	0%
RIESGO DE FRAUDE	28%	28%	28%	16%	100%

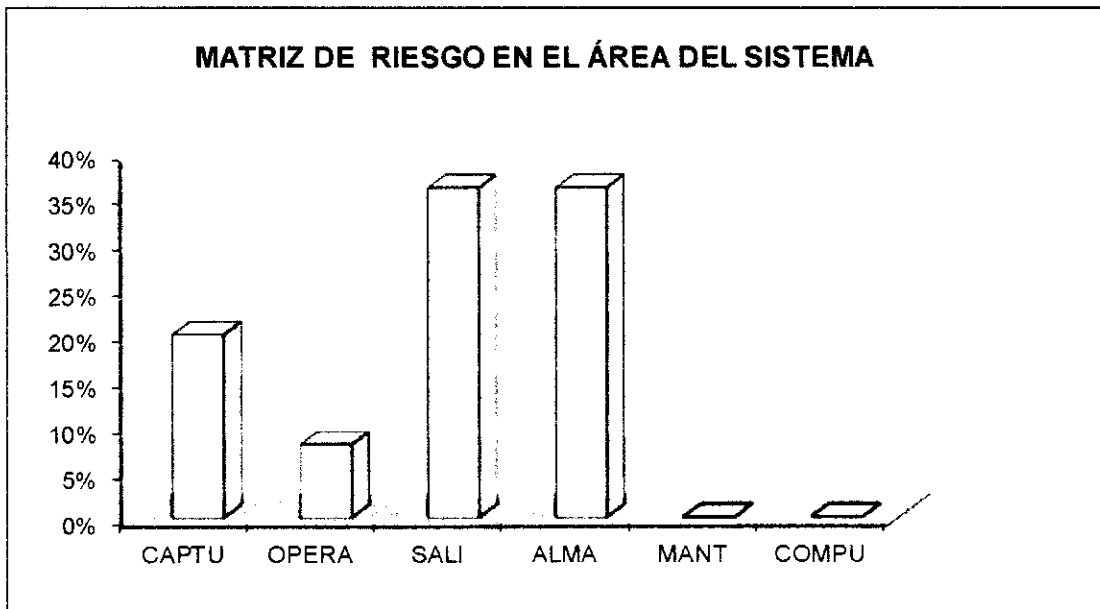
Riesgo de Fraude Informatico

Nulo 0

Bajo 1

Medio 2

Alto 3



ROXALUNA, S.A.

MATRIZ DE EVALUACION DEL RIESGO INHERENTE

AREA DE CUENTAS POR COBRAR

31 DE DICIEMBRE 2013

PT: C/I	Firma	Fecha
Realizó	AP	04/04/2014
Revisó	JCD	04/04/2014

RIESGO O OPORTUNIDAD	RIESGO INHERENTE		RESPUESTA AL RIESGO	
	PROBABILIDAD		RESPUESTA	ALTERNATIVA DE RESPUESTA
<p>La empresa no tiene un control sobre los cheques rechazados, no se registran en la contabilidad; cuando retornan son trasladados a la persona de cobros para que solicite nuevamente un cheque.</p> <p>No existe un procedimiento para los redepósitos. La operación es trabajada por la persona de cobros y la persona encargada de la cuenta de clientes.</p>	A L T A		P R E V E N I R	No permitir que una persona tenga a su cargo la operación completa del departamento de clientes y cobros.
<p>Los abonos parciales que se reciben de los clientes son ingresados al banco y no se registra en la cuenta contable, así como tampoco se afecta el auxiliar. Se le cuestionó al contador y el manifestó que el sistema contable no permite los abonos parciales a las facturas.</p>	A L T A		P R E V E N I R	Todo documento que se reciba en donde se realiza un abono o un cargo a la cuenta de clientes deberá ser registrado en la contabilidad, así mismo, en el auxiliar de clientes deben realizarse los cambios al sistema para que permita los abonos parciales.

ROXALUNA, S.A.

MATRIZ DE EVALUACION DEL RIESGO INHERENTE

AREA DE CUENTAS POR COBRAR

31 DE DICIEMBRE 2013

PT: C/I	Firma	Fecha
Realizó	AP	04/04/2014
Revisó	JCD	04/04/2014

RIESGO O OPORTUNIDAD	RIESGO INHERENTE		RESPUESTA AL RIESGO	
	PROBABILIDAD		RESPUESTA	ALTERNATIVA DE RESPUESTA
Se detectó que no todas las facturas tienen su recibo de caja, en algunos documentos sólo aparece la firma del cobrador o una ilegible de la persona que recibió el pago que indica que ya está cancelado conjuntamente con la fecha.	A L T A		P R E V E N I R	Para que la factura se considere cancelada deberá llevar su respectivo recibo de caja, la firma y el sello de cancelado en la factura, sin embargo, no será suficiente para que se considere pagada.
Se observó que los pagos en efectivo pueden ser recibidos por cualquier persona y no existe ningún procedimiento que indique qué tratamiento se le tiene que dar, se operan igual que un pago con cheque.	A L T A		P R E V E N I R	Los pagos en efectivo tienen que operarse de una forma diferente y no pueden operarse igual que un pago con cheque. El sistema debe tener un ingreso diferente para el efectivo recibido por el pago de las facturas.
La cartera de clientes no es muy grande, sin embargo, no se le envían estados de cuenta a los clientes para confirmar su saldo.	A L T A		P R E V E N I R	Se deberán enviar estados de cuenta a los clientes para la confirmación de saldos cuando los saldos sean mayores a los 90 días o según lo crea conveniente la gerencia.

4.7 INFORME DE AUDITORÍA INTERNA

Guatemala, 15 de abril de 2014

Señores

Junta Directiva

Roxaluna, S.A.

Ciudad de Guatemala

Estimados Señores:

Este informe contiene los resultados de riesgos de fraude informático obtenidos en la revisión del área de cuentas por cobrar. Por lo que no tiene como propósito criticar las actuaciones de funcionarios o empleados involucrados en las operaciones del área auditada, sino que lograr incrementar la eficiencia y rentabilidad de la empresa evitando fraudes

Nuestro estudio y evaluación del sistema de control interno informático sobre riesgos contables de fraude se llevó a cabo con base a cuestionarios de control interno.

La revisión no tuvo ninguna limitación durante su proceso y las discusiones con la administración respecto a los hallazgos que aquí se informan se llevaron a cabo del 01 al 17 de abril del 2014.

A continuación se listan los hallazgos encontrados como resultado de la evaluación practicada, así como sus respectivas recomendaciones en el área de cuentas por cobrar:

ÁREA DE CONTABILIDAD Y CUENTAS POR COBRAR

A. Registro y cobros

Hallazgo:

La empresa no tiene un control sobre los cheques rechazados, no se registran en la contabilidad; cuando retornan son trasladados a la persona de cobros para que solicite nuevamente un cheque.

No existe un procedimiento para los re-depósitos. La operación es trabajada por una persona del cobro y la persona encargada de la cuenta de clientes es la misma.

Recomendación:

No permitir que una persona tenga a su cargo la operación completa del departamento de clientes y cobros. (Ver procedimiento 2 literal A y B)

Hallazgo:

Los abonos parciales que se reciben de los clientes son ingresados al banco y no se registra en la cuenta contable, así como tampoco se afecta el auxiliar. Se le cuestionó al contador y el manifestó que el sistema contable no permite los abonos parciales a las facturas.

Se le preguntó al programador y él confirmó que no se pueden realizar abonos parciales a los documentos de facturación.

Recomendación:

Todo documento que se reciba en donde se realiza un abono o un cargo a la cuenta de clientes deberá ser registrado en la contabilidad. (Ver procedimiento 2 literal C)

Hallazgo:

Se detectó que no todas las facturas tienen su recibo de caja, en algunos documentos sólo aparece la firma del cobrador o una ilegible de la persona

que recibió el pago que indica que ya está cancelado conjuntamente con la fecha.

Recomendación:

Para que la factura se considere cancelada deberá llevar su respectivo recibo de caja, la firma y el sello de cancelado en la factura. (Ver procedimiento 2 literal D)

Hallazgo:

Se observó que los pagos en efectivo pueden ser recibidos por cualquier persona y no existe ningún procedimiento que indique qué tratamiento se le tiene que dar, se operan igual que un pago con cheque.

Recomendación:

Los pagos en efectivo tienen que operarse de una forma diferente y no pueden operarse igual que un pago con cheque. (Ver procedimiento 2 literal E)

Hallazgo:

La cartera de clientes no es muy grande, sin embargo, no se les envían estados de cuenta a los clientes para confirmar su saldo.

Recomendación:

Se deberán enviar estados de cuenta a los clientes para la confirmación de saldos cuando los saldos sean mayores a los 90 días o según lo crea conveniente la gerencia. (Ver procedimiento 2 literal F)

ÁREA DE SISTEMAS

B. Capacitación de ingresos

Hallazgo:

La captura de los datos se realiza desde cualquier terminal, no existe un procedimiento que especifique cómo y quiénes tienen autorización para la

captura, cualquier persona puede acceder sin dejar evidencia de que capturó o alteró la información.

Recomendación:

El acceso al sistema de contabilidad sólo deba realizarse de las terminales asignadas, así como el ingreso al programa mediante clave de acceso de uso exclusivo del departamento de contabilidad. (Ver procedimiento 4 literal B)

Hallazgo:

No existe un reporte de anomalías en datos de entrada, el programador indicó que no se cuenta con ese tipo de reporte. La captura de datos es ingresada en forma empírica, no existen instrucciones por escrito de la forma como se tienen que ingresar los registros.

Recomendación:

El sistema debe emitir un reporte de anomalías, cuando la información que se está ingresado no coincide con la que tiene el programa en su base de datos. (Ver procedimiento 3 literal A)

Hallazgo:

No existe ningún control en la operación del sistema por persona, este tipo de información no la han solicitado nunca, se verificó con el contador, quien indicó que es correcto.

Recomendación:

Toda persona que trabaje en el sistema tiene que tener su clave de acceso y debe quedar la bitácora de las operaciones que realizó en el sistema. (Ver procedimiento 3 literal B)

C. Operación

Hallazgo:

El personal de operadores que trabaja en el control de la información no es rotado, lo que puede permitir que la información sea alterada en una forma fraudulenta.

Recomendación:

Debe rotarse el personal que tiene el control de los registros contables, por lo menos cada seis meses debe existir rotación en este tipo de puestos. (Ver procedimiento 2 literal G)

Hallazgo:

No existe niveles de seguridad en el sistema de información lo que puede ser objeto de fraude, ya que no se cuenta con ningún bloqueo que no permita ingresar a los operadores a áreas que no le fueron asignadas.

Recomendación:

Crear niveles de acceso al sistema. (Ver procedimiento 4 literal B)

Hallazgo:

No hay un lugar adecuado para almacenar la bitácora del sistema lo que puede ser motivo de indicios de alterar las mismas y por consiguiente difícil de controlar un fraude ya ejecutado.

Recomendación:

Los archivos de soporte deben ser almacenados en un lugar físico que tenga las características de seguridad que amerita la información que se guardara. (Ver procedimiento 4 literal C)

D. Salida

Hallazgo:

El no poseer una bitácora en los documentos de salida permite que los informes sean manipulados.

El sistema no tiene un responsable de los documentos de salida lo que no permite que exista un control adecuado de los mismos.

Recomendación:

Elaborar bitácora de documentos de salida, al crear la bitácora se debe tomar en cuenta el usuario que utilizo esta parte del sistema. (Ver procedimiento 3 literal D)

E. Almacenamiento**Hallazgo:**

El sistema no cuenta con claves de acceso que no permita que personas sin autorización ingresen a la información confidencial.

Recomendación:

En las recomendaciones de operación se mencionan crear los niveles de acceso al sistema los mismos deben ser tomados para todas las áreas del programa. (Ver procedimiento 4 literal C)

F. Equipo de cómputo**Hallazgo:**

Los antivirus que están instalados no están actualizados y son obsoletos.

Recomendación:

La actualización inmediata de los antivirus con sus respectivas licencias, los más comerciales en el mercado son los siguientes: Panda, Norton, Symantec y McAfee. (Ver procedimiento 4 literal A)

Hallazgo:

Los controles de acceso al centro de cómputo no existen.

Recomendación:

Aunque el departamento de cómputo es pequeño existen controles mínimos que se deben implementar: (Ver procedimiento 4 literal A)

Deseamos agradecer la colaboración y cortesía mostradas por los funcionarios y empleados, lo cual fue de singular importancia durante el desarrollo de nuestro trabajo.

Dadas las deficiencias y errores suscitados tanto en el diagnóstico y auditoría, proponemos como Auditoría Interna, Procedimientos Informáticos en el Área de Cuentas por Cobrar, que deberán implementarse según autorización de la Gerencia, ante las novedades suscitadas.

Atentamente,

Lic. Adrián Pineda
Auditor Interno
Colegiado 9110728
Roxaluna, S.A.

ROXALUNA, S.A.
PROCEDIMIENTOS INFORMÁTICOS DE
PREVENCIÓN DE FRAUDES EN EL ÁREA DE
CUENTAS POR COBRAR

ÍNDICE	No. de página
1. Introducción	102
2. Objetivo de los procedimientos	103
3. Alcance	103
4. Uso de los procedimientos	103
5. Procedimientos de control interno para la organización del área de contabilidad	104
9. Procedimientos de control interno para el área de cuentas por cobrar	106
10. Procedimientos de control interno de: entrada de datos, el procesamiento de información y la emisión de resultados	109
11. Procedimientos de control interno para la seguridad del área de sistemas.	111
13. Flujogramas	116

INTRODUCCIÓN

Los siguientes procedimientos tienen como objetivo principal, servir como una fuente de consulta y orientación para los responsables del área de cuentas por cobrar.

Para una mejor comprensión los procedimientos, se estructuraron de una manera lógica y sencilla, buscando alcanzar el objetivo para el cual fueron elaborados, sin dejar de ser una herramienta de conocimientos técnicos y administrativos.

Contiene los procedimientos informáticos para cada actividad de forma textual, para las siguientes áreas: área de contabilidad, cuentas por cobrar, entrada de datos en el procesamiento de información y la emisión de resultados y seguridad del área de sistemas

Cabe señalar que los procedimientos estarán sujetos a modificaciones, tanto en las políticas de operación, como en los avances tecnológicos deberán ser revisados por lo menos una vez al año.

PROCEDIMIENTOS INFORMÁTICOS PARA LA PREVENCIÓN DE FRAUDES EN EL ÁREA DE CUENTAS POR COBRAR

OBJETIVO

Servir como instrumento de consulta y apoyo en la prevención de fraudes informáticos de las cuentas por cobrar de la empresa Roxaluna, S.A.

ALCANCE

Lo siguientes procedimientos están dirigidos a todo el personal del área de cuentas por cobrar y demás interesados de la administración.

USO DE LOS PROCEDIMIENTOS

Esta parte del documento proporciona los lineamientos prácticos de las siguientes áreas: contabilidad, cuentas por cobrar, entrada de datos en el procesamiento de información y la emisión de resultados y seguridad del área de sistemas.

Para poder obtener los beneficios deseados de este documento, sus lectores deberán estar familiarizados con las operaciones de la cuenta por cobrar

Si bien, este material resultará útil para aquellos usuarios que pretenden mejorar su control interno en la prevención de fraudes informáticos. Los usuarios deberán guiarse en el contenido del mismo, ya que los procedimientos de control interno informáticos son claramente definidos.

Elaboró Adrián Pineda Guatemala, Abril 2014	Revisó Lic. Juan Carlos Díaz Guatemala, Abril 2014	Aprobó Lic. Antonio Lou Guatemala, Abril 2014
---	--	---

PROCEDIMIENTOS INFORMÁTICOS PARA LA PREVENCIÓN DE FRAUDES EN EL ÁREA DE CUENTAS POR COBRAR

1. Procedimientos de control interno para la organización del área de contabilidad

Objetivo: organizar el área de contabilidad para que funcione con eficacia y eficiencia la empresa, lo cual se logra mediante el diseño adecuado de 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 responsabilidad y la definición clara de los perfiles de los puestos.

Procedimientos a realizar:

- A. Dirección
- B. División del trabajo
- C. Asignación de responsabilidad y autoridad
- D. Establecimiento de estándares y métodos

4.1.1. ASIGNACIÓN

4.1.1.1. DIRECCIÓN

A) Dirección:

Contador General

Coordinación de Recursos: Asignar y distribuir de Manera correcta los recursos del área de contabilidad en la empresas, con el fin de que dichos recursos sean más equitativos y productivos.

Supervisión de Actividades: vigilar que el área contable, sobre la realización de las funciones y actividades que se tienen encomendada, en esta área, supervisar el trabajo que se realiza con los recursos de la empresa.

Elaboró Adrián Pineda Guatemala, Abril 2014	Revisó Lic. Juan Carlos Díaz Guatemala, Abril 2014	Aprobó Lic. Antonio Lou Guatemala, Abril 2014
---	--	---

PROCEDIMIENTOS INFORMÁTICOS PARA LA PREVENCIÓN DE FRAUDES EN EL ÁREA DE CUENTAS POR COBRAR

Delegación de autoridad y responsabilidad: limitar la autoridad y responsabilidad, tanto a los puestos de mayor como de menor jerarquía.

Asignación de actividades: diseñar las actividades de cada uno de los puestos que integran la estructura de la organización.

Distribución de recursos: se debe asignar los recursos disponibles con el propósito de que los empleados cumplan eficientemente con las actividades y tareas que tienen encomendadas.

B) División del Trabajo

Contador General

Se debe realizar La división del trabajo para maximizar la producción de los trabajadores, se deben dividir grandes tareas en lotes más pequeños de trabajo distribuyéndose en varias personas. Con esto se incrementará la eficacia y eficiencia de las actividades de la empresa. Se requiere una división más especializada del trabajo para el cumplimiento de las actividades, operaciones y tareas que se desarrollan.

C) Asignación de responsabilidad y autoridad

Contador General

Se debe asignar las líneas de autoridad por puesto y el establecimiento de los límites de responsabilidad que

Elaboró Adrián Pineda Guatemala, Abril 2014	Revisó Lic. Juan Carlos Díaz Guatemala, Abril 2014	Aprobó Lic. Antonio Lou Guatemala, Abril 2014
---	--	---

**PROCEDIMIENTOS INFORMÁTICOS PARA LA PREVENCIÓN DE FRAUDES
EN EL ÁREA DE CUENTAS POR COBRAR**

tendrá cada uno de estos, incluyendo los canales formales de comunicación. Es delimitar claramente la autoridad y la responsabilidad que tendrá cada integrante de esas áreas.

D) Establecimientos estándares y métodos

Contador General

Se debe estandarizar el desarrollo de todas las actividades y funciones a fin de que estas se realicen de manera uniforme conforme a las necesidades concretas de las unidades que integran la empresa. Se deben establecer de manera uniforme todos aquellos procedimientos y metodologías que permitan estandarizar la operación, así como para el desarrollo de nuevos sistemas de operación.

E) Perfiles de puestos

Contador General

Establecer los requisitos, habilidades, experiencia y conocimientos específicos que se necesita que posea el personal que ocupa un puesto en el área contable.

2. Procedimientos de control interno para el área de cuentas por cobrar

Objetivo: En base a las deficiencias encontradas por la auditoría externa detallar los procedimientos para corregir estas fallas y así evitar algún tipo de fraude.

Procedimientos a realizar:

Elaboró Adrián Pineda Guatemala, Abril 2014	Revisó Lic. Juan Carlos Díaz Guatemala, Abril 2014	Aprobó Lic. Antonio Lou Guatemala, Abril 2014
---	--	---

PROCEDIMIENTOS INFORMÁTICOS PARA LA PREVENCIÓN DE FRAUDES EN EL ÁREA DE CUENTAS POR COBRAR

- A. Cheques rechazados
- B. Separación de funciones
- C. Abonos parciales
- D. Cancelación de facturas
- E. Cobros en efectivo
- F. Emisión de estados de cuenta
- G. Rotación de personal

CONTABILIDAD CONTABILIDAD

A) Cheques rechazados

Auxiliar de Contabilidad I Anular el registro contable realizado al recibir el cheque, de modo que se debite nuevamente la cuenta por caja y bancos y se acredita la cuenta por cobrar por el valor del cheque puesto que no se hizo efectivo el pago. contabilizar la tenencia de ese cheque devuelto hasta que sea entregado al girador o el banco lo pague. Las cuentas de orden contemplan esta situación y para ello ha dispuesto la cuenta, donde se debitará el valor del cheque devuelto y la contrapartida será un crédito a la cuentas deudoras de control por el contra.

B) Separación de funciones

Contador General El departamento de contabilidad debe de dividir las atribuciones de los 2 auxiliares para que no solo uno

Elaboró Adrián Pineda Guatemala, Abril 2014	Revisó Lic. Juan Carlos Díaz Guatemala, Abril 2014	Aprobó Lic. Antonio Lou Guatemala, Abril 2014
---	--	---

PROCEDIMIENTOS INFORMÁTICOS PARA LA PREVENCIÓN DE FRAUDES EN EL ÁREA DE CUENTAS POR COBRAR

realice las operación completa de las cuentas por cobrar. (facturación y de cobros)

C) Abonos parciales

Auxiliar de Contabilidad Los documento que se reciban, en donde se realiza un abono o un cargo a la cuenta de clientes deberá ser registrado en la contabilidad, así mismo, en el auxiliar de clientes, realizar los cambios al sistema para que permita los abonos parciales.

D) Cancelación de facturas

La factura debe de ser cancelada y se emitirá su respectivo recibo de caja, y colocarse la firma y el sello de cancelado en la factura.

E) Cobros en efectivo

Los cobros en efectivo deben de operarse de una forma diferente a los cobros realizados con cheque, se debe de colocar en el recibo de caja que se realizó el cobro en efectivo. Además en el sistema de cómputo deber de tener un ingreso donde haya constancia dicho cobro en efectivo se realizó para el pago de las facturas.

F) Emisión de estados de cuenta.

Elaboró Adrián Pineda Guatemala, Abril 2014	Revisó Lic. Juan Carlos Díaz Guatemala, Abril 2014	Aprobó Lic. Antonio Lou Guatemala, Abril 2014
---	--	---

**PROCEDIMIENTOS INFORMÁTICOS PARA LA PREVENCIÓN DE FRAUDES
EN EL ÁREA DE CUENTAS POR COBRAR**

Emitir estados de cuenta cada mes, deberán de enviarse los mismos a los clientes, para la confirmación de los saldos con la cuenta contable.

G) Rotación de personal

Contador General

Rotar el personal que tiene el control de los registros contables, por lo menos cada año entre los 2 auxiliares que tiene asignados.

3. Procedimientos de control interno de: entrada de datos, procesamiento de Información y la emisión de resultados

Objetivo: se detallaran los procedimientos para verificar la existencia y funcionamiento en la captura de datos; se comprobara que todos los datos sean debidamente procesados y se verificara la confiabilidad, veracidad y exactitud del procesamiento de datos así como en el resultado en la emisión de resultados.

Procedimientos a realizar:

- A. Verificar la existencia y funcionamiento de los procedimientos de captura de datos.
- B. Comprobar que todos los datos sean debidamente procesados.
- C. Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos.
- D. Comprobar la suficiencia de la emisión de información.

Elaboró Adrián Pineda Guatemala, Abril 2014	Revisó Lic. Juan Carlos Díaz Guatemala, Abril 2014	Aprobó Lic. Antonio Lou Guatemala, Abril 2014
---	--	---

**PROCEDIMIENTOS INFORMÁTICOS PARA LA PREVENCIÓN DE FRAUDES
EN EL ÁREA DE CUENTAS POR COBRAR**

A) Verificar la existencia y funcionamiento de los procedimientos de captura de datos

Contador General

Cotejar los datos ingresados, chequeos aleatorios de datos, esto para garantizar la veracidad y confiabilidad de los datos introducidos al sistema.

B) Comprobar que todos los datos sean debidamente procesados

Contador General

Verificar que los datos sean procesados de manera oportuna, confiable, eficiente y que sean procesados sin que sufran ninguna alteración, ya sea accidental, involuntaria o dolosa, durante su procesamiento. Verificar que no haya algún tipo de manipulación externa o interna, accidental o intencional que altere los procesamientos de información implementados en la empresa.

C) Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos.

Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos.

D) Comprobar la suficiencia de la emisión de resultados.

Verificar que la información proporcionada al usuario sea, ni más ni menos, la necesaria para satisfacer sus

Elaboró Adrián Pineda Guatemala, Abril 2014	Revisó Lic. Juan Carlos Díaz Guatemala, Abril 2014	Aprobó Lic. Antonio Lou Guatemala, Abril 2014
---	--	---

**PROCEDIMIENTOS INFORMÁTICOS PARA LA PREVENCIÓN DE FRAUDES
EN EL ÁREA DE CUENTAS POR COBRAR**

requerimientos fundamentales para la realización de sus actividades cotidianas.

4. Procedimientos de control interno para la seguridad del área de sistemas

Objetivo: se detallaran los procedimientos de control interno para la seguridad del área de sistemas, en donde se encuentra la seguridad de sus recursos informáticos, del personal, de la información, de sus programas, detallando las medidas preventivas.

Procedimientos a realizar:

- A. Control para la seguridad física del área de sistemas.
- B. Control para la seguridad lógica de los sistemas.
- C. Control para seguridad de las bases de datos.

Objetivo del control

Medidas preventivas

A) Control para la seguridad física del área de sistemas

Contador General

Inventario del hardware, mobiliario y equipo:

Realizar el registro de carácter contable que se hace de todos los activos de los sistemas, en dicho registro se anotan las características, la configuración, el tipo de procesadores, la velocidad, los componentes, las especificaciones y demás elementos que compone el hardware de cada uno de los sistemas computacionales.

Elaboró Adrián Pineda Guatemala, Abril 2014	Revisó Lic. Juan Carlos Díaz Guatemala, Abril 2014	Aprobó Lic. Antonio Lou Guatemala, Abril 2014
---	--	---

PROCEDIMIENTOS INFORMÁTICOS PARA LA PREVENCIÓN DE FRAUDES EN EL ÁREA DE CUENTAS POR COBRAR

Resguardo del equipo de cómputo: asignar documentalmente el equipo de cómputo, de sus periféricos, mobiliario demás componentes que se hace al personal o a los usuarios del área de sistematización; por medio de estos documentos se les responsabiliza de la salvaguarda y buen uso del equipo que tienen asignado; la intención es contar con un documento de control sobre este tipo de activos y mantenerlo vigente, así como responsabilizar al usuario del uso adecuado y la protección de estos activos.

Bitácoras de mantenimientos y correcciones: hacer el registro pormenorizado y cronológico del mantenimiento preventivo y las reparaciones del hardware, periféricos y equipos asociados del sistema computacional, así como de sus instalaciones y mobiliario; estas bitácoras, una por cada sistema, se obtienen estadísticas útiles para valorar su utilidad en la empresa.

Acceso del personal al área de sistemas: limitar y controlar el ingreso del personal y usuarios al área de sistemas, para evitar contingencias y riesgos físicos a los equipo de dicha área.

Elaboró Adrián Pineda Guatemala, Abril 2014	Revisó Lic. Juan Carlos Díaz Guatemala, Abril 2014	Aprobó Lic. Antonio Lou Guatemala, Abril 2014
---	--	---

**PROCEDIMIENTOS INFORMÁTICOS PARA LA PREVENCIÓN DE FRAUDES
EN EL ÁREA DE CUENTAS POR COBRAR**

Mantenimiento a instalaciones y construcciones: salvaguardar y mantener en buen estado las instalaciones del sistema, ya sean eléctricas, las comunicaciones vía telefónica, satelital, modem u otros medios similares, así como las conexiones del sistema computacional, sean individuales, redes internas, externas, entre otras. Mantenimiento de las construcciones del área de sistemas incluyendo la iluminación, el medio ambiente el clima artificial para la comodidad de los usuarios, etc.

Actualización, asesoría y mantenimiento del hardware: hacer convenios con los proveedores, distribuidores de equipos y demás personas involucradas en el buen funcionamiento del hardware, periférico, mobiliario y equipo del área de sistemas. Incluyendo la asesoría, actualización de sistemas, los avances tecnológicos y demás aspectos que permiten el uso óptimo del sistema.

B) Control para la seguridad lógica de los sistemas

Acceso al sistema, a los programas y a la información: delimitar el nivel de acceso de los usuarios y personal al área de sistemas, estableciendo los privilegios, modos de entrada, forma de uso del sistema y otras características, para el control de los

Elaboró Adrián Pineda Guatemala, Abril 2014	Revisó Lic. Juan Carlos Díaz Guatemala, Abril 2014	Aprobó Lic. Antonio Lou Guatemala, Abril 2014
---	--	---

**PROCEDIMIENTOS INFORMÁTICOS PARA LA PREVENCIÓN DE FRAUDES
EN EL ÁREA DE CUENTAS POR COBRAR**

usuarios. Creando claves de acceso y delimitación del uso del programa e información.

Establecimiento de niveles de acceso: definir mediante la programación y las paqueterías específicas de control lógico, los límites de acceso de los usuarios a los programas institucionales, paqueterías y herramientas de desarrollo, de acuerdo con la importancia del software e información que pueden manejar.

Dígitos verificadores y cifras de control: se debe hacer el establecimiento de operaciones aritméticas, controles sumados y dígitos de verificación matemática de los datos que se capturan y se procesan en el sistema, con el propósito de mantener la confiabilidad de estos últimos.

Palabras clave de accesos: establecer por medio de palabras clave (contraseñas) para el acceso y uso de los programas y archivos de información. Estas claves las debe establecer el administrador del sistema y por el propio usuario.

C) Control para seguridad de las bases de datos.

Programas de protección para impedir el uso inadecuado y la alteración de datos de uso

Elaboró Adrián Pineda Guatemala, Abril 2014	Revisó Lic. Juan Carlos Díaz Guatemala, Abril 2014	Aprobó Lic. Antonio Lou Guatemala, Abril 2014
---	--	---

PROCEDIMIENTOS INFORMÁTICOS PARA LA PREVENCIÓN DE FRAUDES EN EL ÁREA DE CUENTAS POR COBRAR

exclusivo: definir el usuario autorizado que tenga acceso a los datos de uso exclusivo. Esto se hace para proteger la información contenida en los archivos del sistema.









Respaldo periódicos de información: establecer los planes y programas de respaldo (back-up) de la información de la base de datos, de la información de cada usuario, de las diferentes áreas o de toda la institución. Los archivos de respaldo deben de tener 2 copias de respaldo una que debe estar en las instalaciones de la empresa y la otra deberá estar en una cajilla de seguridad.

Planes y programas para prevenir contingencias y recuperar información: salvaguardar las bases de datos de la institución.

Control de acceso a las bases de datos: Limitar el acceso de usuario no autorizados a las bases de datos.

Elaboró Adrián Pineda Guatemala, Abril 2014	Revisó Lic. Juan Carlos Díaz Guatemala, Abril 2014	Aprobó Lic. Antonio Lou Guatemala, Abril 2014
---	--	---

**PROCEDIMIENTOS INFORMÁTICOS PARA LA PREVENCIÓN DE FRAUDES
EN EL ÁREA DE CUENTAS POR COBRAR**

SIMBOLO	SIGNIFICADO
Archivo 	Archivo temporal o definitivo de algún documento
Documento 	Documento generado o requerido por el procedimiento Cuando existen copias se pueden representar y enumerar asignando al original indistintamente la letra O o el número 1 y al duplicado y demás copias la numeración correlativa
Terminal 	Identifica el inicio y el fin de un procedimiento según la palabra que se utilice dentro del óvalo
Actividad 	Representa una actividad la cual se describe brevemente dentro del rectángulo
Conector 	Indica continuidad de una acción con otra dentro de una misma página
Líneas de Flujo 	Conectan elementos del procedimiento e indican la secuencia a seguir
Conector de Página 	Conecta una actividad con otra de una página diferente Opcionalmente se puede colocar el número de la página a la que se conecta
Decisión 	Señala un punto en el proceso en el que hay que tomar una decisión. A partir de allí el procedimiento puede tomar dos (2) vías y la selección de una de ellas depende de la respuesta a la pregunta que se describe dentro del rombo

Elaboró Adrián Pineda Guatemala, Abril 2014	Revisó Lic. Juan Carlos Díaz Guatemala, Abril 2014	Aprobó Lic. Antonio Lou Guatemala, Abril 2014
---	--	---

**PROCEDIMIENTOS INFORMÁTICOS PARA LA PREVENCIÓN DE FRAUDES
EN EL ÁREA DE CUENTAS POR COBRAR**

DESCRIPCION	VENTAS	CONTABILIDAD	COBROS	MENSAJERO
1. Inicio de proceso	Inicio de proceso			
2. Ventas elabora cotización para cliente	Elabora cotización			
3. Ventas emite Orden de facturación y traslada a contabilidad	Emite orden de facturación			
4. Contabilidad crea código de cliente		Creación de código de cliente		
5. Contabilidad elabora e imprime factura		Elabora e imprime factura		
6. Contabilidad contabiliza factura, registra auxiliar de clientes y traslada factura a cobros		Contabiliza y registra auxiliar		
7. Cobros adjunta documentación y entrega factura a mensajero para entregar a cliente			Adjunta documentación y entrega al mensajero	
8. Mensajero entrega factura a cliente				Entrega factura a cliente

Elaboró Adrián Pineda Guatemala, Abril 2014	Revisó Lic. Juan Carlos Díaz Guatemala, Abril 2014	Aprobó Lic. Antonio Lou Guatemala, Abril 2014
---	--	---

**PROCEDIMIENTOS INFORMÁTICOS PARA LA PREVENCIÓN DE FRAUDES
EN EL ÁREA DE CUENTAS POR COBRAR**

DESCRIPCION	VENTAS	CONTABILIDAD	COBROS	MENSAJERO
9. Mensajero entrega copia de factura firmada por cliente a cobros				Entrega copia de factura a cobros
10. Cobros recibe copia de factura y registra en cuentas por cobrar			Recibe copia de factura y registra en cuentas por	
11. Cobros, transcurrido el tiempo de crédito, procede a realizar el cobro			Procede a realizar el cobro	
12. Cobros, procede a realizar llamadas a clientes para verificar pago.			Confirma pago	
			Si	Realiza de nuevo gestión de cobro
13. Se procede a realizar el cobro			Procede a realizar el cobro	
14. Cliente realiza pago				Recibe cheque del cliente, emite recibo de caja
15. Mensajero entrega cheque de pago a cobros				Entrega cheque de pago a cobros
16. Cobros recibe pago y deposita en cuentas bancarias			Recibe pago y deposita	
17. Cobros da de baja a cliente del reporte de cuentas por cobrar			Da de baja a clientes del reporte de cuentas por	
18. Fin del proceso			Fin del proceso	

Adrián Pineda
Guatemala, Abril 2014

Lic. Juan Carlos Díaz
Guatemala, Abril 2014

Lic. Antonio Lou
Guatemala, Abril 2014

CONCLUSIONES

1. La empresa de transporte de la unidad de análisis, dentro de su actividad productiva es la prestación de servicios, cuenta en la actualidad con un sistema informático para el manejo de clientes, no confiable en un 100% basado en el informe elaborado por auditoria externa y como consecuencia de ello, está expuesta a riesgo y pueda tener dificultades de índole operacional, financiero y contable que pueda obstaculizar el logro de sus objetivos.
2. La elaboración e implementación de procedimientos de control interno informáticos proporcionará mayor seguridad a la empresa, determinando la certeza que la información contable, contenida en la base de datos es real y que no fue manipulada o alterada mediante fraude informático.
3. El sistema informático que actualmente posee la empresa unidad de estudio, se encuentra estructurado en módulos que permiten trabajar independiente a los distintos departamentos, así hay un módulo de contabilidad, etc., y particularmente el módulo de clientes, lo que es considerado en el ámbito de informática como una ventaja, sin embargo, dicho sistemas ha puesto al descubierto su vulnerabilidad, pues a pesar de poseer medidas de seguridad propias de los sistemas de cómputo, estas demostraron no ser suficientes ante las habilidades del personal involucrado en las alteraciones, que al final resultaron en detrimento de los intereses de la compañía.
4. Para la empresa de transporte unidad de estudio, el fraude informático, es algo que se puede prevenir pero el riesgo siempre existirá. Con la implementación de nuevos controles mejorará los ya existentes, se va a tener la seguridad que se minimizará el riesgo de la comisión de hechos delictivos.

RECOMENDACIONES

1. La empresa de transporte objeto de estudio debe de mantener en el área de clientes un adecuado sistema informático que le sirva a la administración como un medio valioso y de ayuda en la toma de decisiones, veraz, completa y oportuna.
2. Para obtener mayor seguridad las empresas y así prevenir fraudes informáticos, específicamente en el área de clientes o cuentas por cobrar, deberán de implementar los procedimientos de control interno informático.
3. La empresa unidad de estudio no debe de confiar plenamente en los dispositivos de seguridad que de fábrica tengan el sistema de cómputo. Por el contrario, deben de hacerse las pruebas necesarias sobre la seguridad del sistema e implementar sus propios mecanismo de rastreo, monitoreo o supervisión de la actividad de los usuarios dentro del modulo de cuentas por cobrar del sistema de computo. Además debe de apoyarse en la auditoría interna para mitigar el riesgo de fraude que requiere de procedimiento de prevención y controles que en su conjunto reduzcan la probabilidad de ocurrencia de fraudes y conductas impropias, pero que al mismo tiempo maximicen la posibilidad de detectarlas antes de que signifiquen un quebranto económico para la organización.
4. Implementar los procedimientos de control interno para prevenir el fraude informático específicamente en el área de clientes de la empresa objeto de estudio, para mejorar los ya existentes, y así tener la seguridad de minimizar el riesgo de la comisión de hechos delictivos.

REFERENCIAS BIBLIOGRÁFICAS

1. Balcarcel Osoy, Juan Fernando. (2012). El Contador Público y Auditor en su Calidad de Auditor Interno en el diseño de Procedimientos de Prevención de Fraude en el Módulo de Créditos del Sistema Informático para un Banco Privado. México.
2. Colegio Contadores Públicos y Auditores de Guatemala. (2008). Código de Ética Profesional. Guatemala.
3. Comité de Normas Internacionales de Contabilidad. (2010-2011). NIFF para PYMES.
4. Instituto para el Desarrollo del Auditor Interno, (2006). Seminario Fraude corporativo, prevención y detección, Guatemala. Pàg.68
5. Comité Internacional de Prácticas de Auditoría. (2013). Normas Internacionales de Auditoría (NIA).
6. Congreso de la República de Guatemala, Decreto número 2-70, Código de Comercio y sus Reformas.
7. Congreso de la República de Guatemala, Decreto 17-73, Código Penal y sus Reformas.
8. Congreso de la República de Guatemala, Decreto 51-92, Código Procesal Penal y sus reformas.
9. Estupiñan, Rodrigo. (2003) Control Interno y Fraudes, Ecoe Ediciones Bogotá, Colombia. Pag.360
10. E. Koler, Erick L. (1999). Diccionario para Contadores, Editorial HispanoAmericana,S.A. de C.V. UTEHA, México Pàg.717
11. Editores Salvat- (2004). Material de apoyo de definiciones. Editores. Colombia, Impreso por Printer Colombina, S.A. - 16,000 P.
12. Mora, José Luis. (2000). Introducción a la Informática. México Editorial Trillas. Universidad Autónoma de México,
13. Muñoz Razo, Carlos. (2002) Auditoría en Sistemas Computacionales. Primera Edición, México , Pearson Educación,

14. Perdomo Salguero, Mario Leonel. (2009). Procedimientos y Técnicas de Auditoría I con Base en NÍAS. - Tercera edición. - Ediciones Contables, Administrativa. - Guatemala, 219 P.
15. Real Academia Española. (2001). Diccionario de la Lengua Española. - Vigésima segunda edición. - España, - www.rae.es.
16. Universidad de San Carlos de Guatemala, (2002). Facultad de Ciencias Económicas, Escuela de Auditoría. Material de apoyo El control interno. Guatemala,
17. Tiznado, Marco Antonio. (2004) Informática. Segunda Edición, México, McGraww-Hill Interamericana,

Webgrafía

18. Alegsa, (2014). Diccionario de informática y tecnología. Obtenido el 02-03-2015. www.alegsa.com.ar
19. Universidad Tecnológica de México, (2013). El contador público y auditor como auditor interno. Obtenido el 02-04-2015. <http://www.utem.cl/oferta-academica/oferta-academica-diurna/contador-publico-y-auditor/>
20. Universidad del salvador (2014). El Auditor Interno. Obtenido el 02-02-2014. <http://www.biblioteca.utec.edu.sv>
21. Cerna Apaza Luis Alfonso (2006). Fraude y error en auditoria. Universidad Nacional de Ciencias Económicas de Perú. Obtenido el 06-10-2006. <http://aprendeonline.udea.edu.co/index.php/adversia/article/download/4770/4185>
22. Superintendencia de Administración Tributaria. (2014). Leyes y Reglamentos. Obtenido el 10-01-2014. www.sat.gob.gt
23. Real Academia Española. (2014). Diccionario y Ortografía. Obtenido 12-03-2014. www.rae.com
24. Asociación de Examinadores de Fraude Certificados. (2014). Análisis de los Fraudes. Obtenido el 19-01-2014. www.acfe.com

25. Lefcovich Mauricio León. (2014). Mejora Continua y Evaluación de Control. Interno. Obtenido el 07-02-2014. <http://www.gerencie.com/auditoria-interna.htm>,
26. Universidad Tecnológica de Panamá. (2014). Ingeniería de Sistemas Computacionales. Obtenido el 13-02-2014. <http://www.utp.ac.pa/objetivos-y-funciones-direccion-de-auditoria-interna-y-transparencia>
27. Instituto Internacional de Auditoria Interna Argentina. (2004) La Ética y los códigos de Ética del Auditor Interno. Obtenido el 28-01-2014. <http://www.laauditoriainterna.org/-y-el-control-interno.html>
28. The Institute of Internal Auditors. (2014) Normas Internacionales para el Ejercicio Profesional de la Auditoria Interna. Obtenido 15-03-2014. www.theiia.org
29. IIA-Guatemala (2014) Obtenido el 26-03-2014 . Noticias y Certificaciones. http://www.theiia.org/chapters/index.cfm?act=home_page&cid=331

ANEXO
GLOSARIO

Glosario de términos informáticos

Antivirus: software que se instala en el computador para detectar y eliminar virus informáticos.

Backup: también llamado *copia de seguridad*, es la tarea de duplicar y guardar cualquier tipo de datos o información en otro lugar (disco, servidor...) para que pueda ser recuperado en caso de la pérdida de la información original.

Bluetooth: sistema de conexión inalámbrica para voz y datos. Es utilizado en distancias cortas. Su límite de acción es de unos 10 metros.

Browser: programa o aplicación que permite navegar en Internet y encontrar exactamente la información o temática que se busca. Las más populares son: Chrome, Firefox, Safari y Explorer.

Caché: memoria existente en el disco duro que permite guardar copias temporales de archivos para poder acceder a ellos en ciertos momentos. Es útil cuando se accede a Internet, ya que se pueden guardar algunos elementos de páginas Web para no tener que cargarlos en la próxima visita a la misma página.

Cookie: pequeño fichero que se instala en la memoria virtual del computador cuando se accede a páginas Web. Sirve para que la página visitada conozca el perfil de sus visitantes y guardar contraseñas.

Download: *descarga*. Se refiere al proceso de transferir datos desde un punto remoto (servidor u otro computador) a tu propio equipo.

Hardware: se refiere a la parte física o sólida de un ordenador u otro elemento informático.

Formatear: es el proceso de preparar tu disco duro para que se pueda instalar el sistema operativo.

Interface: punto de comunicación entre dos elementos electrónicos o informáticos. Muchas veces se refiere a él como *puerto*. También se podría definir como el punto de contacto entre el usuario, el computador y el programa; por ejemplo, el teclado o un menú.

Microprocesador: componente de hardware que contiene un sólo circuito integrado que lleva a cabo instrucciones.

Modem: dispositivo que sirve para conectar con Internet. Lo que hace es modular los datos digitales para su transmisión por líneas telefónicas convencionales, para después remodular la señal a su llegada.

Sistema informático: conjunto de elementos hardware, software y periféricos que conectados entre sí, forman un computador.

Sistema operativo: conjunto de programas que sirven para manejar un computador.

Software: conjunto de programas, procedimientos y documentación asociados a un sistema informático.

Contraseña: es una cadena de caracteres con la que se restringe o permite el acceso, de ciertos usuarios, a un determinado lugar o fichero. El ejemplo más habitual es la contraseña de una tarjeta de crédito.

Gusano (Worm): Es un programa similar a un virus que, a diferencia de éste, solamente realiza copias de sí mismo, o de partes de él.

Hacker: Persona que accede a un ordenador de forma no autorizada e ilegal.

Herramienta de hacking: Programa que puede ser utilizado por un *hacker* para causar perjuicios a los usuarios de un ordenador (pudiendo provocar el control del ordenador afectado, obtención de información confidencial, chequeo de puertos de comunicaciones).

Troyano / Caballo de Troya: En sentido estricto, un troyano no es un virus, aunque se considere como tal. Realmente se trata de un programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad del usuario afectado. La historia mitológica *El Caballo de Troya* ha inspirado su nombre.

Troyano bancario: Programa malicioso, que utilizando diversas técnicas, roba información confidencial a los clientes de banca y/o plataformas de pago online.

Vacunación: Es una técnica antivirus que permite almacenar información sobre los ficheros, con el fin de detectar posibles infecciones de éstos, posteriormente.

Virus: Los virus son programas que se pueden introducir en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.

Vulnerabilidades: Fallos o huecos de seguridad detectados en algún programa o sistema informático, que los virus utilizan para propagarse e infectar.