UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

"METODOLOGÍA PARA LA IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN RELEVANTES EN UNA AUDITORÍA DE ESTADOS FINANCIEROS"

Trabajo de investigación presentado por:

Guardado Quintanilla, Manuel Antonio

Guzmán Sosa, Ludwig Javier

Montiel Hernández, Oscar Alcides

Para optar al grado de:

LICENCIADO EN CONTADURÍA PÚBLICA

Febrero 2014

San Salvador, El Salvador, Centroamérica

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

Rector	:	Ingeniero Mario Roberto Nieto Lovo
Secretaria General	:	Doctora Ana Leticia Zavaleta de Amaya
Decano de la Facultad de Ciencias Económicas	:	Máster Roger Armando Arias Alvarado
Secretario de la Facultad de Ciencias Económicas	:	Máster José Ciriaco Gutiérrez Contreras
Directora de la Escuela de Contaduría Pública	:	Licenciada María Margarita de Jesús Martínez Mendoza de Hernández
Coordinador de Seminario	:	Licenciado Mauricio Ernesto Magaña Menéndez
Asesor Director	:	Licenciado Daniel Nehemías Reyes López
Jurado Examinador	:	Licenciado Daniel Nehemías Reyes López
	:	Licenciado Adilso Alberto Rogel Pineda
	:	Licenciado Juan Francisco Guardado Escobar

Febrero 2014

San Salvador, El Salvador, Centroamérica

AGRADECIMIENTOS

En primer lugar, agradezco a DIOS Todopoderoso por su bendición y amor incondicional a lo largo de mi vida y por haberme permitido alcanzar esta meta. A mis padres María Ana Quintanilla de Guardado y José Lisandro Guardado por su amor, apoyo, esfuerzo y sacrificio. A mis hermanas y hermanos por todo su apoyo. A mis compañeros Ludwig Javier Guzmán Sosa y Oscar Alcides Montiel Hernández por haber depositado en mí la confianza para poder culminar con este proyecto. Y a todos aquellos amigos, amigas, seres queridos y docentes que me han apoyado y contribuido en el logro de esta meta.

Manuel Antonio Guardado Quintanilla

Doy gracias a Dios por ofrecerme la maravillosa oportunidad de concluir con mi educación superior, por su infinito e incondicional apoyo recibido en toda mi vida. También expreso mi gratitud a todas aquellas personas que directa o indirectamente han colaborado en mi formación profesional a lo largo de todos estos años: mis padres, familia, profesores y compañeros.

Ludwig Javier Guzmán Sosa

Agradezco a DIOS todopoderoso por brindarme la vida, la salud, el tiempo para lograr esta grata meta y por permitirme contar con los recursos para dedicarme a este cometido. Doy las gracias a mi familia, a mis padres Berta Alicia Hernández y José Oscar Montiel Benítez por mostrarme valores como el trabajo y la humildad, a mis compañeros de grupo y a todas las personas y profesionales que estuvieron a mi lado apoyándome en todo momento.

Oscar Alcides Montiel Hernández

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El presente trabajo de graduación surge con base a las necesidades existentes en las firmas de auditoría de El Salvador, de contar con un modelo, metodología o estándar para poder identificar y valorar los riesgos relevantes de tecnología de información (TI) en una auditoría de estados financieros.

El auditor se ha visto en la necesidad de poseer el conocimiento suficiente de los sistemas de información por computadora para: planear, dirigir, supervisar y revisar el trabajo a desarrollar, ello debido a la creciente disponibilidad de información electrónica y procesos automatizados por recursos informáticos y de tecnologías de comunicación, que son capaces de satisfacer las circunstancias tanto funcionales como económicas, de oportunidad y efectividad de las entidades o empresas que las utilizan; de tal manera que hemos llegado a un momento en que la TI constituye un eje fundamental en las entidades. Por lo que tales circunstancias requieren que el contador público esté preparado para actuar en dos áreas: la auditoría y la informática.

Como aporte social, se diseñó una propuesta que tiene por objetivo principal el desarrollar una metodología para la identificación y evaluación de riesgos sobre control interno informático relevante en la información financiera y está encaminado a servir como herramienta de apoyo en la fase de planeación de auditoría a las firmas de El Salvador. En el documento se proponen criterios técnicos para el entendimiento del ambiente y control interno de TI en el negocio, basados en COBIT 5 y se brindan herramientas para identificar riesgos con base a las debilidades del control interno, que impacten en la información financiera de las entidades como apoyo al profesional para el diseño de un enfoque global de la naturaleza, oportunidad y extensión de los procedimientos a incorporar en la planeación de una auditoría de estados financieros mediante una matriz de evaluación de riesgos.

La investigación se desarrolló bajo el tipo de estudio hipotético deductivo ya que este permite la formulación de hipótesis, las cuales son confrontadas con los hechos reales. El método utilizado para la obtención de información fue mediante encuestas a los encargados de auditoría, de las firmas con personería jurídica autorizadas por el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría (CVPCPA), utilizando la técnica de muestreo aleatorio simple, dando como resultado un tamaño de la muestra de 59 firmas, con un universo de 308.

De esta forma, la indagación permitió establecer las conclusiones y recomendaciones siguientes: Las firmas de auditoría se ven en dificultades al momento de ejecutar una evaluación de control interno a las TI relevante a la información financiera conforme a normativa debido a que el material con el que cuentan es insuficiente. Generalmente dichas entidades presentan en su equipo de trabajo poca o nula capacitación sobre aspectos relacionados al área de tecnologías de información. Por lo tanto, se recomienda hacer uso de la presente metodología, la cual detalla la forma de cómo identificar y evaluar riegos cuando la información financiera se encuentra bajo un ambiente de sistemas computarizados y a los gremios comprometidos con la profesión de contaduría pública y auditoría impartir seminarios y capacitaciones para mejorar las competencias relacionadas con la informática.

INTRODUCCIÓN

En las últimas décadas la humanidad ha experimentado cambios sustanciales en sus formas de comunicación y procesamiento de la información, por medio de tecnologías inimaginables a principios del siglo XX. La informática abarca a ritmo acelerado muchas áreas del acontecer empresarial, incluida su información financiera. El profesional de la contaduría que prepara y audita los estados financieros, tiene la obligación técnica de aplicar y conocer estas vertiginosas evoluciones, para aprovechar las ventajas competitivas resultantes de su uso, e igualmente importante, en la comprensión de los efectos nocivos que concurren dentro de la información financiera, denominados de aquí en adelante como riesgos TI.

Estos riesgos para ser considerados requieren habilidades adicionales a la contabilidad, la falta de una educación continuada limita el alcance de un auditor para actuar convenientemente según la complejidad del sistema de información administrada y controlada por las entidades, esto crea una disparidad de las destrezas necesarias con respecto a las requeridas.

El presente documento ha sido elaborado con el fin de reducir la brecha existente entre, los conocimientos recomendados internacionalmente para un adecuado análisis del riesgo que incide en la información financiera, y las capacidades actuales - determinadas en la investigación – que poseen los profesionales. Se pretende lograr con la elaboración de una propuesta, creada en forma de guía, dirigida hacia los auditores de estados financieros, permitiéndoles cumplir con los requerimientos establecidos en la NIA 315, en cuanto a identificar y evaluar riesgos informáticos.

El trabajo que a continuación se expone está distribuido en cuatro capítulos, el primero presenta un marco conceptual incluyendo los principales antecedentes de la auditoria y el marco de control COBIT, define y clasifica los conceptos generales relacionados a controles y riesgos de información automatizada, así como tipos de metodologías para evaluar riesgos, por último detalla el contenido técnico y legal utilizada para sustentar la investigación.

En el capítulo dos, se contempla la metodología bajo la cual se realizó la investigación de campo, los resultados de tal indagación son analizados y presentados al lector, se define el tipo de estudio, la determinación de la muestra y los instrumentos y técnicas de recolección de información, las que dan como resultado un diagnóstico que muestra las dificultades actuales del auditor para considerar estos tipos de

riesgos, al momento de establecer una respuesta global a los mismos y determinar la naturaleza, oportunidad y extensión de los procedimientos sustantivos.

En el capítulo tres, se desarrolla un caso práctico definiendo en primer lugar una descripción general de la metodología que contiene una serie de pasos elaborados para el entendimiento de la entidad y su control interno de conformidad a lo establecido en las NIA's y tomando como base las mejores prácticas de control según COBIT 5.

Para finalizar se muestra en el capítulo IV, las principales conclusiones sobre la problemática encontrada y las recomendaciones a los principales sectores que se relacionan con esta investigación.

CAPÍTULO I: MARCO TEÓRICO, CONCEPTUAL Y LEGAL

1.1 Antecedentes

1.1.1 Antecedentes de la auditoría.

En El Salvador la auditoría financiera surge en 1939 por medio del establecimiento inicial regulatorio a la carrera contable, esto se da a través de la ley aprobada el 21 de Septiembre de 1940 según decreto 57 publicado en el diario oficial el 15 de octubre del mismo año; por medio de él fue creado el Consejo Nacional de Contadores Públicos.

Para el año 1967 se facultó al Ministerio de Educación el otorgamiento de la calidad de Contador Público Certificado (CPC). Así mismo, se destaca como factor relevante la carrera de contaduría pública en la Universidad de El Salvador, lo cual ofreció al profesional un enfoque de estudio superior dando paso a la creación de los contadores públicos académicos (CPA), los cuales ejercieron labores de auditorías financieras en forma independiente.

En los años 90's los gremios de contadores públicos unificaron sus esfuerzos y realizaron varias convenciones nacionales, como resultado surgieron las Normas de Contabilidad Financiera (NCF). En el año 2000 se da una importante reforma legal en el ámbito de la profesión de la Contaduría Pública, en el Código de Comercio, Ley del Registro de Comercio, Ley de la Superintendencia de Obligaciones Mercantiles y la creación de la Ley Reguladora del Ejercicio de la Contaduría y Auditoría, posteriormente se emite el Código Tributario.

Entre estas reformas y creaciones de ley se destaca, en cuanto a la contabilidad y la auditoría, lo establecido en los artículos 443 al 444 del Código de Comercio y el articulo 36 literales f, g y h de la Ley Reguladora del Ejercicio de la Contaduría, en donde se adoptan las Normas Internacionales de Contabilidad y de Auditoría sugeridas por los organismos internacionales IFRS e IFAC respectivamente.

El Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría acordó que las Normas Internacionales de Información Financiera (llamadas antes NIC) deben ser las bases contables a utilizar en la preparación de los estados financieros de propósito general en El Salvador; así mismo, aprobó un plan escalonado de implementación durante los años de 2004 al 2006. El 22 de diciembre de 2004, el referido

Consejo acordó establecer un marco de referencia que se denomina Normas de Información Financiera adoptadas en El Salvador, el cual contemplaba las Normas Internacionales de Contabilidad, revisiones y/o actualizaciones, incluyendo las respectivas interpretaciones, vigentes hasta el 31 de octubre de 2003.

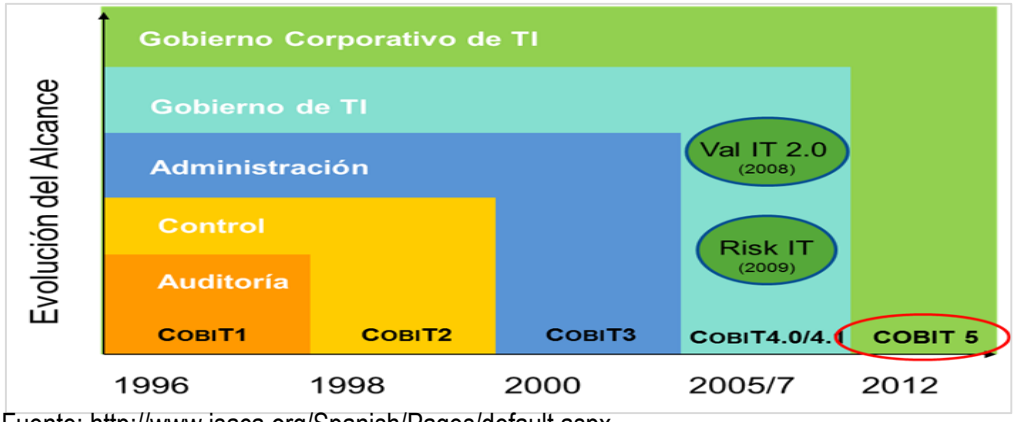
1.1.2 Antecedentes de COBIT

Con el inicio de la revolución industrial surgió la necesidad de controlar las operaciones que por su magnitud eran realizadas por máquinas dirigidas por operarios. Por lo tanto se cree que el origen del control interno sucedió a fines del siglo XIX, debido a que los hombres de negocios se preocuparon por formar y establecer sistemas adecuados para la protección de sus intereses. En forma general, el crecimiento económico de los negocios, implicó una mayor complicación en las empresas y por consecuencia en su administración.

El marco de buenas prácticas **COBIT** se emprendió por primera vez en el año 1995, con el propósito de fundamentar un mayor beneficio global que pudiese tener un impacto duradero sobre el campo de visión de los negocios, en especial sobre los controles de los sistemas de información. La primera versión fue publicada en 1996 y se distribuyó en 98 países de todo el mundo. La segunda en abril de 1998, desarrolló y mejoró lo que poseía la anterior mediante la asociación de un mayor número de documentos de referencia, nuevos y revisados objetivos de control de alto nivel, intensificando las líneas maestras de auditoría, introduciendo un conjunto de herramientas de implementación.

En su cuarto ejemplar, se cubren 210 objetivos de control clasificándolos en cuatro dominios: planificación y organización, adquisición e implementación, entrega y soporte, y, supervisión y evaluación.

Figura 1. Evolución del alcance de COBIT



Fuente: http://www.isaca.org/Spanish/Pages/default.aspx

La edición COBIT 5 lanzada en el año 2012, proporciona una visión empresarial del gobierno de TI que presenta a la tecnología e información como protagonistas en la creación de valor para las empresas. Se basa en COBIT 4.1, y a su vez lo amplía mediante la integración de otros importantes marcos y normas como Val IT y Risk IT, Information Technology Infrastructure Library (ITIL ®) y las normas ISO relacionadas.

1.2 Conceptos

A continuación se detallan los principales conceptos que están directamente relacionados con la investigación.

Control interno: es el proceso diseñado, implementado y mantenido por los responsables del gobierno de la entidad, la dirección y otro personal, con la finalidad de proporcionar una seguridad razonable sobre la consecución de los objetivos de la entidad relativos a la fiabilidad de la información financiera, la eficacia y eficiencia de las operaciones, así como sobre el cumplimiento de las disposiciones legales y reglamentarias aplicables.[1]

Control interno informático COBIT: conocido antiguamente como Objetivos de Control para Tecnologías de Información o Relacionadas; usado actualmente solo como un acrónimo en su quinta revisión. Un marco completo, internacionalmente aceptado, para el gobierno y la gestión de la información de la empresa y la tecnología de la información que soporta a los ejecutivos de la empresa y los gestores en la definición y consecución de las metas de negocio y las metas relacionadas.[2]

Desarrollo profesional continuo: constituyen estados fijos o inmutables, actividades de aprendizaje que permiten a los contadores desarrollar y mantener las capacidades para desenvolverse con competencia en sus entornos técnicos. Este pensamiento tiene como meta cultivar y mantener la competencia después de la calificación profesional. Esto implica el desarrollo de las capacidades mediante programas de formación

---

[1] Federación Internacional de Contadores (IFAC por sus siglas en inglés). Normas Internacionales de Auditoría y Control de Calidad No. 315, párrafo 4C. Edición 2011.

[2] Asociación de Auditoría y Control de Sistemas de Información (ISACA por sus siglas en inglés), *"*COBIT 5 u*n marco de negocio para el gobierno y la gestión de TI de la empresa".* Pág. 90, Edición 2012.

formales y verificables (a veces denominados en conjunto "formación profesional continua" o FPC) o a través de una actividad de aprendizaje no formalizada.[3]

Procedimientos de valoración del riesgo: procedimientos de auditoría aplicados para obtener conocimiento sobre la entidad y su entorno, incluido su control interno, con el objetivo de identificar y valorar los riesgos de incorrección material, debida a fraude o error, tanto en los estados financieros como en las afirmaciones concretas contenidas en éstos.

Riesgo informático: se refiere a la incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos.

Tecnología de información y comunicación: término de uso general que hace referencia a todos los elementos que se encuentren involucrados en torno al ordenador (computadora), entre ellos se destacan el hardware y el software.

1.3 Clasificación

1.3.1 Clasificación de la auditoría[4]

Existen muchos tipos de auditoría, pero dentro de todas ellas se mencionan las siguientes:

Por su lugar de origen

Esta se refiere a la forma en que se realiza este tipo de trabajos y también como se establece la relación laboral en las empresas donde se llevará a cabo.

a) Externa: este tipo de auditoría la realizan auditores totalmente ajenos a la empresa, por lo menos en el ámbito profesional y laboral. Algunos autores lo asemejan con la de estados financieros, debido a que ofrecen fe pública de las opiniones efectuadas sobre la razonabilidad de las cifras expresadas en los mismos, y cuya característica esencial es que no reciben indicaciones, en cuanto a su actuación profesional, de ningún nivel jerárquico dentro de la organización auditada; limitándose en última instancia

---

[3] Federación Internacional de Contadores (IFAC por sus siglas en inglés). *Normas Internacionales de Formación (IES 2*), pág.11, Edición 2008.

[4] Muñoz Razo, Carlos. (2002). "*Auditoría en Sistemas Computacionales"* Primera Edición. Estado de México, México. Pearson Educación de México, S.A. de C.V., Prentice-Hall. Pág. 12.

al compromiso explícito de proporcionar un dictamen a la medida de las necesidades de la entidad. En este sentido, es importante destacar que esta clasificación puede adoptar una diversa gama de revisiones y pertenecerán únicamente cuando no exista una vinculación de beneficios a los empleados de corto plazo tales como sueldos, salarios, aportaciones a la seguridad social, etc.

b) Interna: la relación de trabajo es directa y subordinada a la institución donde se ejecutará la revisión.

Por su área de aplicación

Se enfocan al ámbito específico donde se llevan a cabo las actividades y operaciones que serán auditadas.

a) Financiera: es la revisión de los estados financieros de una entidad económica, cuyo objetivo es expresar una opinión independiente sobre la razonabilidad de las cifras presentadas en ellos.
b) Fiscal: evaluación que se realiza a las empresas con el fin de emitir una opinión relacionada al cumplimiento de las obligaciones tributarias formales y sustantivas de los contribuyentes.
c) Administrativa: examen sistemático, exhaustivo que se realiza a la actividad administrativa de una entidad, en cuanto a su organización, las relaciones entre sus integrantes, el cumplimiento de las funciones y actividades que regulan sus operaciones.
d) Integral: evaluación exhaustiva, sistemática y global a todas las actividades y operaciones de una entidad.
e) Informática: el propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la entidad.
f) Ambiental: revisión que se hace de la calidad del aire, la atmósfera, el ambiente, las aguas, ríos, lagos, océanos, así como de la conservación de la flora y la fauna silvestre, con el fin de dictaminar sobre las medidas preventivas, o en su caso correctivas que disminuyan y eviten la contaminación.

1.3.2 Clasificación de los controles de TI

Cuando son diseñados, desarrollados e implementados deben ser completos, simples, fiables, adecuados y rentables, evaluando siempre el costo-beneficio. Históricamente, los controles relativos a la informática se han clasificado de la siguiente manera:

a) **Preventivos:** los destinados en evitar anticipadamente el surgimiento de sucesos indeseables, tales como software de seguridad que impida los accesos no autorizados al sistema.

b) **Detectivos:** conjunto de procedimientos encaminados en identificar eventos no deseados en el momento que suceden. Entre ellos se encuentra la bitácora de registro de intentos no autorizados y el registro de la actividad diaria para detectar errores u omisiones.
c) **Correctivos:** aquellos mecanismos encargados en revertir el efecto ocasionado por los eventos no deseados. Un control común de este tipo es aquel encargado en la recuperación de un archivo dañado a través de la copia de seguridad o backup.

1.3.3 Clasificación de los riesgos.

a) **Inherente:** tendencia de un área de tecnología de información a cometer un error que podría ser material, en forma individual o en combinación con otros, suponiendo la inexistencia de controles internos relacionados. Entre ellos se encuentra el riesgo asociado a la seguridad del sistema operativo, representado por cambios no autorizados en los parámetros de configuración y acceso.
b) **De control:** situación en donde un error, que podría cometerse individualmente o combinado con otros, no pueda ser evitado y corregido oportunamente por el sistema de control interno. Este tipo de riesgos puede estar asociado a las revisiones manuales de registros, los cuales son normalmente altos, debido a que las actividades que requieren investigación a menudo se pierden con facilidad por el volumen de información registrada.
c) **De detección:** el que se produce cuando los procedimientos sustantivos del auditor no detectan un error que podría ser material, individualmente o en combinación con otros. Dentro de estos se encuentran los riesgos asociados a la identificación de violaciones de la seguridad en un sistema de aplicación, debido a que en el transcurso de la auditoría, los registros de todo su período no se encuentran disponibles. Estos se encuentran asociados con la falta de procedimientos dirigidos a la recuperación ante desastres, dado que su existencia puede verificarse con facilidad.

Controles internos para contrarrestar el riesgo de fraude

La información es el recurso más importante en toda área informática, por esta razón es de suma importancia aquellos controles que se encuentren establecidos para minimizar los efectos del fraude o manipulación de datos. La seguridad del control debe existir en distintos aspectos tales como los accesos al sistema, los resultados obtenidos y el procesamiento de los datos. Estos controles se presentan en forma de procedimientos, técnicas y métodos de prevención.

Los controles informáticos son clasificados en generales y de aplicación, en la tabla 1 se encuentra cada uno de ellos debidamente explicado:

Tabla 1. Controles informáticos

Categorías de los controles generales y de aplicación		
Tipo de control	**Categoría de control**	**Ejemplo de control**
Controles generales	Administración de la función de TI	El jefe de tecnología de información (CTO por sus siglas en inglés) reporta a la alta administración y al consejo.
	Separación de responsabilidades de TI	Se separan las responsabilidades de programación, operaciones y control de información
	Desarrollo de sistemas	Los equipos de usuarios, analistas de sistemas y programadores desarrollan y prueban perfectamente el software
	Seguridad física y en línea	Se restringe el acceso al hardware. Las contraseñas y las identificaciones de usuario limitan el acceso al software y a los archivos de información, la encriptación y los firewall protegen de personas externas la información y los programas
	Respaldo y planeación de contingencias	Constantemente en el año se preparan y prueban los planes escritos de respaldo
	Controles de hardware	La falla en la memoria o en el disco duro origina mensajes de error en el monitor
Controles de aplicación	Controles de entradas	Las pantallas formateadas de antemano muestran los datos del personal que deberán ingresarse
	Controles de procesamiento	Las pruebas de razonabilidad revisan los precios unitarios de venta utilizados para procesar la venta
	Controles de salidas	El departamento de ventas desarrolla una revisión posterior al procesamiento de las operaciones de venta

Fuente: Alvin A. Arens, Randal J. Elder, Mark S. Beasley. (2007). "Auditoría un Enfoque Integral". 11ª Edición. México. Pearson Educación de México, S.A. de C.V., Prentice-Hall. (Página 349).

1.3.4 Clasificación de los riesgos de incorrección material

Existen dos principales categorías de este tipo de amenazas presentes en los estados financieros, ellos son los errores y el fraude, a continuación se muestra una breve descripción de los mismos:

Errores

Son las omisiones o inexactitudes en los estados financieros de una entidad, para uno o más periodos, resultantes de un fallo al emplear información que estaba disponible en el periodo que fueron realizados. Algunos de los más comunes en los estados financieros son:

a) Errores aritméticos
b) Errores en la aplicación de políticas contables
c) Inadvertencia o mala interpretación de hechos.

Fraude

Son todas aquellas omisiones o inexactitudes que en forma intencional afectan los estados financieros de una entidad. A su vez, se clasifica en los siguientes conceptos:

- Información financiera fraudulenta.

Son aquellas omisiones o inexactitudes expresadas en los estados financieros con el propósito de engañar a los usuarios. En mayor medida, estos fraudes son relacionados en el importe del saldo de ciertas cuentas más que de las revelaciones.

- Apropiación indebida de activos

Implica la sustracción de los activos de una entidad específica, que por lo general es desarrollado por parte de empleados y la dirección. Puede adoptar diversas modalidades, tales como: malversación de ingresos, sustracción de activos físicos de la entidad, uso de los activos de la empresa para uso personal.

Ambos tipos de fraude obedecen a la existencia de tres condiciones en particular, que al cumplirse, facilita la aparición de estas inexactitudes en la información. El primero de ellos son los incentivos/presiones, los cuales son categorizados como un beneficio esperado por aquellos posibles actores fraudulentos; el segundo se representa por la oportunidad, a través la viabilidad de cometer el hecho la administración y/o empleados pueden considerar la posibilidad de realizarlo; y el tercero bajo la figura de actitudes/racionalización, que constituye la existencia de un carácter o conjunto de doctrinas que conlleva al sujeto a desarrollar un fraude.

1.4 Características de los controles de tecnología de la información[5]

El control interno de TI, debe cumplir al menos con las siguientes características:

a) **Oportuno:** es la esencia del control y consiste en que los resultados obtenidos por su aplicación sean percibidos justo a tiempo.

b) **Cuantificable:** toman valores numéricos y/o porcentuales, de tal manera que se pueda conocer el grado de cumplimiento de los resultados obtenidos contra los resultados esperados en algún momento futuro.

c) **Calificable:** medibles en términos de cualidad, los cuales pueden ser aplicados para identificar el grado de cumplimiento que posean en cuenta los resultados esperados.

d) **Confiable:** los controles deben ofrecer resultados correctos, libres de cualquier error, alteración o desviación.

e) **Estándares y normas de evaluación:** deberán compararse con algún marco de referencia de alguna normativa previamente establecida. Esto permite una estandarización y una adecuada apreciación de los valores obtenidos.

1.5 Principales riesgos de tecnología de información.

a) Generales

El fácil acceso a la información, debido al rápido avance de la tecnología ha generado que las entidades hagan un uso más frecuente de la informática, por lo cual se han presentado situaciones tales como:

- Problemas de confidencialidad: accesos no autorizados a información confidencial, para obtener copias piratas de programas, modificar datos de aplicaciones ya sea en provecho propio o como sabotaje, modificación de datos (como nóminas, expedientes, destrucción de información).
- Utilización indebida del ordenador: juegos, trabajos particulares y/o para otra entidad.

---

[5] Muñoz Razo, Carlos. (2002). "*Auditoría en Sistemas Computacionales"* Primera Edición. Estado de México, México. Pearson Educación de México, S.A. de C.V., Prentice-Hall. Pág. 102

- Caídas o congelamiento de los sistemas, si un sistema de información deja de funcionar, se crea normalmente un gran problema que puede ser tan grave que lleve a la paralización completa de operaciones en una organización.
- Dependencia de sistemas o programas que procesen los datos de una manera no exacta o que procesen datos no exactos, o ambas cosas.
- La posibilidad de que personal de TI obtenga privilegios de acceso más allá de los necesarios para desempeñar sus deberes asignados, faltando, por lo tanto, a la segregación de deberes.
- Cambios no autorizados a datos en los archivos maestros [6]

b) Relevantes para una auditoría de estados financieros

Si bien la informática puede reforzar el control interno de una compañía, también puede afectar su riesgo de control global. Muchos asociados con los sistemas manuales se reducen y en algunos casos se eliminan. Sin embargo, se crean nuevas amenazas y pueden dar paso a importantes pérdidas si son ignoradas. Una debilidad inminente es la incapacidad para recuperar registros importantes producidos por la falla en los sistemas de información, o el uso de datos no confiables debido a errores de procesamiento a causa de dicha tecnología, podría paralizar a las organizaciones. Estos riesgos aumentan la probabilidad de errores importantes en los estados financieros que debe considerar la administración, y sobre todo el auditor.[7] A continuación se presentan los principales riesgos importantes específicos al área de TI importantes en una auditoría de estados financieros, estructurados bajo los componentes comunes de una auditoría de sistemas como:

- **Niveles de seguridad**

Física: sin una apropiada protección física, el hardware o el software pueden no funcionar. Por consiguiente, es importante proteger al hardware y al software de forma física y proteger de algún daño físico a la

[6] Cornejo Pérez, Mario Hernán. "Tecnología de información en el contexto profesional del contador público", en R*evista Ábaco Contable,* (San Salvador, No. 2, 2008), pág. 4.

[7] Alvin A. Arens, Randal J. Elder, Mark S. Beasley. (2007). "*Auditoría un Enfoque Integral."* Decimoprimera edición. Estado de México, México. Pearson Educación de México, S.A. de C.V., Prentice-Hall. Pág. 347.

información relacionada que pudiera resultar del uso inapropiado, sabotaje, o daño causado por el medio ambiente (como fuego, calor, humedad o agua).

Pistas de auditoría: dado que la mayoría de la información se introduce directamente a la computadora, la tecnología a menudo reduce o incluso elimina los documentos de origen y los registros que permiten a la organización rastrear la información contable. A estos documentos y registros se les llama registro de auditoría.

Acceso no autorizado: con frecuencia, los sistemas de contabilidad basados en TI permiten el acceso en línea a la información en archivos maestros y otros registros guardados de forma electrónica. Dado que el acceso en línea puede ocurrir en forma remota desde varios puntos, incluso por personas externas con acceso remoto a través de internet, existen posibilidades de un acceso ilegítimo.

Separación de tareas menores: a medida que las organizaciones convierten sus procesos manuales a computarizados, las computadoras ejecutan muchas tareas que tradicionalmente estaban separadas, tales como la autorización y la teneduría de libros. Por lo tanto, la combinación de actividades de diferentes partes de la organización centraliza las responsabilidades que antes por costumbre estaban divididas. El personal con acceso al software y a los archivos maestros podría estar en posibilidades de robar activos a menos que las principales funciones estuvieran separadas de forma adecuada.

- **Percepción de usuarios**

Reducción de la participación humana: en la mayoría de los entornos informáticos, los empleados que manejan el proceso inicial de las operaciones nunca ven los resultados finales. Por lo cual, son los menos capaces de percibir los errores. Pero incluso si vieran los resultados, sería difícil apreciar las fallas dado que éstos se presentan sumamente resumidos.

- **Funcionamiento**

Errores sistemáticos contra errores al azar: a medida que las organizaciones reemplacen los procedimientos manuales por procedimientos basados en la tecnología, disminuirán los riesgos de errores aleatorios. Sin embargo, la incidencia de un error sistemático se incrementa dada la uniformidad del

procesamiento de las computadoras. Una vez que los procedimientos se programan en un software de cómputo, éste procesa la información de forma consistente para todas las operaciones hasta que los procedimientos programados se cambian. No obstante, los defectos de programación de software y cualquier cambio en ella afectan la confiabilidad en el procesamiento computarizado, lo que origina varios errores importantes.

Entrada de datos: es común que en los sistemas avanzados de TI, ciertos tipos de operaciones sean iniciadas de forma automática por la computadora. Como es el caso del cálculo de intereses para las cuentas de ahorro y el pedido de inventario cuando se alcanza el nivel preestablecido para hacerlo.

- **Planes de contingencia**

Pérdida de información: la mayoría de la información básica en un entorno tecnológico se guarda en archivos electrónicos centralizados. Cuando ésta se centraliza, aumenta el riesgo de pérdida o destrucción de archivos completos con severas consecuencias. Existen posibilidades de error en los estados financieros y en ciertos casos, la organización podría sufrir serias interrupciones en el negocio.

Necesidad de experiencia en TI: incluso cuando las compañías compran sistemas de cómputo relativamente sencillos que incluyen el software, es indispensable contar con personal con suficiente conocimiento y experiencia para instalarlo, mantenerlo y utilizarlo. A medida que el uso de estos recursos se incremente en las organizaciones, se necesitarán especialistas calificados. Muchas corporaciones crean una función completa del personal que incluye a los programadores, operadores, supervisores de redes, responsable de los archivos, especialistas en aseguramiento de calidad y administradores de bases de datos. Otras entidades contratan externamente la administración de las operaciones del sistema de información.

1.6 Tipos de metodologías para evaluación de riesgos.

Todas las metodologías desarrolladas y utilizadas en la auditoría y el control interno, se pueden agrupar en dos grandes familias, estas son:[8]

[8] Velthius Mario Piattini, Navarro Emilio del Peso, Ruiz Mar del Peso (2008). "*Auditoría de Tecnología y Sistemas de Información". Madrid, España. RA-MA Editorial. Pág. 60.*

1.6.1 Metodología cuantitativa.

Diseñadas para producir una lista de riesgos que pueden compararse entre sí con facilidad por tener asignados valores numéricos. Estos valores en el caso de metodologías de análisis de riesgos o de planes de contingencia, son datos de probabilidad de ocurrencia (riesgo) de un evento y que se deben extraer de un registro de incidencias donde el número de ellas tienda al infinito o sea suficiente grande. Entre los coeficientes más usados se encuentra el llamado "ALE" (Annualized Loss Expentacy), expectativa de pérdida anual, resultado de multiplicar la pérdida máxima posible de cada bien o recurso por la amenaza con probabilidad más alta.

Este modelo tiene dos inconvenientes principales, la primera es la debilidad de los datos de la probabilidad de ocurrencia y por los pocos registros de incidentes y la segunda es la dificultad de evaluar económicamente todos los impactos que pueda acaecer.

1.6.2 Metodología cualitativa.

Se refiere a la utilización de formas descriptivas para presentar la magnitud de consecuencias potenciales y la posibilidad de ocurrencia. Se diseñan escalas ajustadas a las circunstancias de acuerdo a las necesidades particulares de cada organización o el concepto particular del riesgo evaluado.

Para el análisis de la probabilidad, se deben establecer las categorías a utilizar y la descripción de cada una de ellas, con el fin de que cada persona que aplique la escala mida a través de ella los mismos ítems:

- ALTA: es muy factible que el hecho se presente.
- MEDIA: es factible que el hecho se presente.
- BAJA: es muy poco factible que el hecho se presente.

Para el análisis del impacto, el mismo diseño puede aplicarse para la escala de medida cualitativa, estableciendo las categorías y la descripción, así:

- ALTO: los niveles de impacto/efecto son elevados para la entidad. De tal manera que las operaciones normales del negocio podrían verse suspendidas o paralizadas.
- MEDIO: cuando el nivel de impacto tiene consecuencias moderadas a la institución. A través de costos económicos considerables pero sin detener el curso normal de las actividades empresariales.

- BAJO: en donde el efecto presenta resultados bajos o imperceptibles hacia la entidad. Presentados comúnmente como aquellos aspectos en donde el nivel de riesgo identificado es aceptable por parte de la administración y auditor.

1.7 Ventajas y limitantes en la consideración de riesgos informáticos en una auditoría de estados financieros.

1.7.1 Ventajas

La información obtenida al momento de considerar estos riesgos pueden proporcionar las siguientes ventajas para el auditor de estados financieros:

Establece incongruencias entre la estrategia existente en las tecnologías de información que posee la entidad y sus estrategias del negocio de acuerdo a COBIT 5; sustenta valoraciones de riesgos de incorrección material, relativas al uso de hardware y software según NIA 315; obtiene evidencia de auditoría acerca de la eficacia operativa de los controles internos relacionadas a la información financiera e identifica inconsistencias debidas a errores o fraude informáticos.

En la planeación

En la identificación de las áreas en las que puede resultar necesaria una consideración especial de la auditoría; por ejemplo, en la adecuación de la aplicación, por parte de la dirección, de la hipótesis de empresa en funcionamiento, o en la consideración de la finalidad empresarial de las transacciones.

Dentro de la fase de planeación se observan las siguientes ventajas al considerar los riesgos de tipo informático:

a) Ayudan en la correcta determinación del alcance de los procedimientos sustantivos según NIA 300.
b) Mejoran la eficiencia en el proceso de auditoría, en el sentido de realizar aquellos procedimientos suficientes de acuerdo al sistema informático del cliente conforme a NIA 300.
c) Priorizan áreas que ostenten debilidades de control interno relacionadas al computador.

1.7.2 Limitantes

Sin la adecuada consideración de este tipo de riesgos, que tienen impacto significativo en las cifras presentadas en los estados financieros, los auditores financieros poseen dificultades para cumplir la base técnica establecida en las Normas Internacionales de Auditoría; al omitir la evaluación de las áreas críticas,

debilidades o riesgos de informática, el trabajo del profesional queda limitado a confiar, dar por correctos o creer en el funcionamiento de los controles generales y de aplicación de los sistemas computacionales.

Por otro lado, el auditor que excluye estos riesgos en el desarrollo de la fase de planeación de auditoría, está imposibilitado de comunicar las debilidades del control interno que puedan existir a nivel informático; asimismo carece de las herramientas para detectar la presencia, ocurrencia o hechos relacionados con las representaciones erróneas de importancia relativa debido a fraude o error.

1.8 Principales respuestas a la evaluación de riesgos en tecnologías de información

Debido a que las amenazas reales informáticas se presentan en forma compleja y son difíciles de predecir se vuelve necesario considerar metodologías para medirlas eficazmente. Aunque estas que se relacionan con análisis de riesgos se utilizan desde los años 80, los registros estadísticos de incidentes son escasos y por tanto el riesgo científico de los cálculos probabilísticos es pobre.

La adecuada identificación y evaluación de los riesgos informáticos permite tomar acciones tales como: evitarlos, transferirlos, reducirlos y asumirlos. Los tres primeros van acompañados de actuaciones traducidas por medio de controles o contramedidas, el último mencionado es lo que se hace si no se controla el riesgo en absoluto. A continuación se amplía sobre las posibles respuestas a los riesgos identificados:

a) Evitarlos: apartarse, alejarse, excluir la situación o evento que generar el riesgo cuando sea posible, a través de la instalación de un nuevo sistema contable, porque se conoce que posee errores o fallas.
b) Transferirlos: trasladar o compartir la amenaza con otros, tal como adquirir equipo informático bajo la figura de arrendamiento financiero, para cargar al arrendatario las posibles pérdidas por obsolescencia.
c) Reducirlos: minimizar, mitigar o disminuir el riesgo, por medio de la adquisición de licencias de software antivirus, firewall, antispyware para contrarrestar los efectos de los virus, spyware, ataques externos, software malicioso.
d) Asumirlos: aceptar el riesgo, cuando el gobierno corporativo considera que la situación como esta es la mejor alternativa, representado comúnmente en la negativa de recibir soporte técnico y/o actualizaciones de seguridad, mejoras a los sistemas de uso de oficina para hojas de cálculo, presentaciones, sistemas contables computarizados, por la decisión de la administración de usar software sin licencia cuando el auditor desconoce de TI.

1.9 Base técnica

En la tabla 2 se muestran los aspectos técnicos relacionados a la identificación y evaluación de riesgos al sistema de información en el proceso de una auditoría de estados financieros.

Tabla 2. Aspectos técnicos relacionados a la identificación y evaluación de riesgos de TI en el proceso de una auditoría de estados financieros.

Base técnica	Descripción	Fecha de vigencia
Norma Internacional de Formación No. 2 (IES 2): contenido de los programas profesionales de formación en contaduría.	Esta normativa prescribe el marco de referencia de los programas profesionales de formación en contaduría que los aspirantes deben adquirir para ser calificados como contadores profesionales. Como objetivo principal, establece que los aspirantes a participar en un organismo miembro de IFAC posean conocimientos contables avanzados suficientes para poder actuar como contadores profesionales competentes en un entorno cada vez más complejo y cambiante. De acuerdo a esta normativa, el conocimiento principal en los programas profesionales de formación en contaduría puede dividirse en tres aspectos importantes: a) contaduría, finanzas y conocimientos relacionados; b) conocimiento organizacional y de negocios; y c) conocimiento de tecnología de la información y competencias.	01 de enero del 2005.
Declaración Internacional de Prácticas Educativas No. 2 (IEPS 2): tecnología de la información para contadores profesionales	Desarrolla, amplía y estructura los principales conocimientos para darle cumplimiento a la IES 2, en el aspecto “conocimiento de tecnología de información y competencias”, suministra una dirección para los organismos miembros de la IFAC y otros educadores en la implementación en relación a los componentes de conocimientos informáticos de los programas educativos de contabilidad profesional precalificada.	01 de octubre de 2007.
Objetivos de Control para Tecnologías de Información o Relacionadas (COBIT 5). Un marco de negocio para el	Describe cinco principios y siete catalizadores que dan soporte a las empresas en el desarrollo, implementación, mejora continua y	2012

Base técnica	Descripción	Fecha de vigencia
gobierno y la gestión de las TI de la empresa	supervisión de buenas prácticas relacionadas con el gobierno y la gestión de TI Se basa en cinco principios: 1. Satisfacer las necesidades de las partes interesadas 2. Cubrir la empresa extremo a extremo 3. Aplicar un marco de referencia único integrado 4. Hacer posible un enfoque holístico 5. Separar el gobierno de la gestión Siete catalizadores: 1. Procesos 2. Información 3. Estructuras organizativas 4. Principios, políticas y marcos 5. Cultura, ética y comportamientos 6. Personas, habilidades y competencias 7. Servicios, infraestructura y aplicaciones	
Normas Internacionales de Auditoría		
NIA	**Descripción**	**Fecha de vigencia**
240: responsabilidades del auditor en la auditoría de estados financieros con respecto al fraude	Esta norma trata el modo de aplicar la NIA 315 y la NIA 330 en relación con los riesgos de incorrección material debidos al fraude	15 de diciembre de 2009.
265: comunicación de las deficiencias en el control interno a los responsables del gobierno y a la dirección de la entidad	Trata de la responsabilidad que tiene el auditor de comunicar adecuadamente, a los responsables del gobierno de la entidad y a la dirección, las deficiencias en el control interno que haya identificado durante la realización de la auditoría de los estados financieros.	15 diciembre de 2009.

Base técnica	Descripción	Fecha de vigencia
	Al realizar la identificación y valoración del riesgo de incorrección material el auditor debe obtener conocimiento del control interno relevante para la auditoría	
300: planificación de la auditoría de estados financieros	Menciona la responsabilidad del auditor en desarrollar un plan de auditoría, el cual debe incluir una descripción de: a) la naturaleza, el momento de realización y la extensión de los procedimientos planificados para la valoración del riesgo, como determina la NIA 315 b) la naturaleza, el momento de realización y la extensión de procedimientos de auditoría posteriores planificados relativos a las afirmaciones, tal como establece la NIA 330	15 diciembre de 2009.
315: identificación y valoración de los riesgos de incorrección material mediante el entendimiento de la entidad y de su entorno	Trata de la responsabilidad que tiene el auditor de identificar y valorar los riesgos de incorrección material en los estados financieros, mediante el conocimiento de la entidad y de su entorno, incluido el control interno de la entidad. El sistema de información, incluidos los procesos de negocio relacionados, relevante para la información financiera y la comunicación, entre el entorno de TI relevante para la auditoría el auditor puede considerar los siguientes: 1. Un sistema de información está constituido por una infraestructura (componentes físicos y de hardware), software, personas, procedimientos y datos. Muchos sistemas de información hacen un amplio uso de las tecnologías de la información (TI). 2. El sistema de información relevante para los objetivos de la información financiera, que incluye el sistema de información financiera, engloba los métodos y registros que: • identifican y registran todas las transacciones válidas; • describen las transacciones oportunamente con suficiente grado de detalle para permitir su correcta clasificación a efectos de la información financiera;	15 de diciembre de 2009.

Base técnica	Descripción	Fecha de vigencia
	• miden el valor de las transacciones de un modo que permite que su valor monetario correcto se registre en los estados financieros; • determinan el periodo en el que se han producido las transacciones con el fin de permitir su registro en el periodo contable correcto; • presentan adecuadamente las transacciones y la correspondiente información a revelar en los estados financieros. 3. La calidad de la información generada por el sistema influye en la capacidad de la dirección de tomar las decisiones adecuadas en materia de dirección y control de las actividades de la entidad, así como de preparar informes financieros fiables. 4. La comunicación, que implica proporcionar conocimiento de las funciones y responsabilidades individuales del control interno sobre la información financiera, puede adoptar la forma de manuales de políticas, manuales contables y de información financiera y circulares. La comunicación también puede ser realizada por vía electrónica, verbal y a través de las actuaciones de la dirección.	
330: respuestas del auditor a los riesgos valorados	Menciona el diseño e implementación de respuestas a los riesgos de incorrección material identificados y valorados por el auditor de conformidad con la NIA 315	15 de diciembre de 2009.
620: utilización del trabajo de un experto	Trata de las responsabilidades que tiene el auditor respecto del trabajo de una persona u organización en un campo de especialización distinto al de la contabilidad o auditoría, cuando dicho trabajo se utiliza para facilitar al auditor la obtención de evidencia de auditoría suficiente y adecuada.	15 de diciembre de 2009.

Fuente: elaboración propia.

1.10 Base legal

La tabla 3 presenta aquellos aspectos legales relacionados con la auditoría.

Tabla 3. Aspectos legales relacionados con la auditoría.

Base legal	Descripción	Fecha de vigencia
Ley Reguladora del Ejercicio de la Contaduría Pública y Auditoría	Tiene por objeto regular el ejercicio de la profesión de la contaduría pública, la función de auditoría y los derechos y obligaciones de las personas naturales o jurídicas que las ejerzan.	Abril de 2000.
Código de Comercio	Menciona en el art. 290 que la vigilancia de los contadores públicos será ejercida por un consejo de vigilancia que tendrá la organización y atribuciones que dicha ley le confiera.	Mayo de 1970.
Código Tributario y su Reglamento de Aplicación	Código Tributario El Art.107 permite el uso de sistemas computarizados para la emisión de tiquetes en sustitución de factura, así mismo, en la elaboración de documentos electrónicos (formulario único). Es mencionada en el Art.113 las normas administrativas sobre la emisión de documentos, en la que facilitan la sustitución de los formularios manuales por formularios electrónicos. Dentro del Art.115 se expone la necesidad de solicitar autorización a la administración tributaria sobre el uso de sistemas computarizados para la emisión de tiquetes en sustitución de facturas. Establece en su Art.139 que la contabilidad podrá llevarse en forma manual o mediante sistemas computarizados.	Enero de 2001.

Base legal	Descripción	Fecha de vigencia
	Los registros que deben llevar los contribuyentes del IVA son detallados en el Art.140, en él menciona que pueden ser llevados a través de sistemas mecanizados o computacionales de contabilidad Así mismo, el art. 147 hace referencia a que cuando la contabilidad sea llevada en forma computarizada, deberán conservarse los medios magnéticos que contengan la información, al igual que los respectivos programas para su manejo por un lapso de diez años. El Art.173 estipula que la administración tributaria tiene facultades de fiscalización, inspección, investigación y control sobre los sistemas de facturación autorizados por tal institución gubernamental. Reglamento de aplicación del Código Tributario Según el Art. 115, se debe colocar el cartel de autorización junto a la maquina en un lugar visible, consignar las series de tiquetes en la declaración de IVA y emitir un resumen diario de las operaciones. Debera realizarse el reporte de ventas totales diario (total z) y parcial (total x), especificando los requisitos del articulo 45 del Reglamento de aplicación del Código Tributario así también deberán coincidir con el Libro de Ventas a Consumidor Final y conservarse por cuatro años. Art. 147 CT.	

Fuente: elaboración propia.

CAPÍTULO II: METODOLOGÍA DE INVESTIGACIÓN

2.1 Tipo de estudio

El tipo de estudio se realizó en base al método hipotético deductivo ya que este permite la formulación de hipótesis, las cuales son confrontadas con los hechos reales, éstas plantean la relación entre dos variables y además proponen un sentido de entendimiento entre ellas. Por lo anterior se pretende explicar y describir si en la actualidad existe alguna forma de identificar y evaluar los riesgos de control interno de las tecnologías de información que inciden en la información financiera y como esta impacta en la planeación de una auditoría externa.

2.2 Unidad de análisis

Para la investigación, el estudio se dirigió a los auditores que laboran en las firmas con personería jurídica de El Salvador y que prestan servicios de auditoría financiera, con el propósito de recabar información en cuanto a la inexistencia de procedimientos para la identificación y evaluación de los riesgos informáticos en la fase de planeación.

2.3 Universo y muestra

2.3.1 Universo

Estuvo conformado por las personas jurídicas ubicadas en El Salvador dedicadas a la prestación de servicios de auditoría, las cuales de conformidad al registro manejado por el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría (CVPCPA), representan un total de 308 al 31 de enero de 2013. (Ver anexo 1)

2.3.2 Muestra

De acuerdo al universo establecido se empleó una muestra probabilística tomando en cuenta una población finita, desarrollada sobre la base de procedimientos estadísticos. Para la selección de la muestra se utilizó el método aleatorio simple, que consiste en que todos los elementos de la población tienen la misma probabilidad de ser escogidos.

Determinación de la muestra

La muestra se determinó mediante la siguiente fórmula:

$$n = \frac{Z^2.\,\mathrm{p}.\,\mathrm{q}.\,\mathrm{N}}{(\mathrm{N}-1).\,e^2 + Z^2.\,\mathrm{p}.\,\mathrm{q}}$$

Dónde:

n = Tamaño de la muestra

N = Tamaño de la población

Z = Valor crítico correspondiente a un coeficiente de confianza con el cual se desea hacer la investigación. (Para una confianza del 95%, Z = 1.96)

p = Probabilidad de ocurrencia del evento (95% ≡ 0.95)

q = Probabilidad de no ocurrencia del evento (1 – p ≡ 1 - 0.95 = 0.05)

e = Error máximo tolerable (5% ≡ 0.05)

Por lo tanto:

$$n = \frac{(1.96)^2.\,(0.95).\,(0.05).\,(308)}{(308-1).\,(0.05)^2 + (1.96)^2.\,(0.95).\,(0.05)}$$

$$n = \frac{56.202608}{0.7675 + 0.182476}$$

$$n = \frac{56.202608}{0.949976}$$

$\boldsymbol{n = 59.1621346223}$ **Aproximado $\boldsymbol{n}$ = 59**

2.4 Instrumentos y técnicas de investigación

El instrumento utilizado fue la encuesta con preguntas cerradas y abiertas dirigidas especialmente a auditores para obtener información que contribuyó al diagnóstico de la investigación, de las firmas con personería jurídica de El Salvador.

Dentro de las técnicas utilizadas se encuentran: el análisis bibliográfico el cual consiste principalmente en la recopilación y clasificación de la información existente contenida en libros, tesis, folletos, sitios web, entre otros. Con el fin de adquirir el conocimiento teórico básico para la investigación; y finalmente, la observación con la cual se pretendió que la investigación de campo llegase a comprobar que ocurre con la identificación y evaluación de riesgos de TI en la fase de planeación de las auditorías de estados financieros por parte de las unidades de análisis.

2.5 Recolección de información

2.5.1 Investigación documental o bibliográfica

El objetivo de esta fase fue determinar, los aspectos generales y específicos del tema, por medio de la revisión bibliográfica existente. La información recolectada a través de esta técnica es el punto inicial de la investigación y juega un papel importante para el lector, en el entendimiento de la diversidad de definiciones, para complementar el trabajo de campo.

2.5.2 Investigación de campo

En esta etapa se ejecutó el instrumento detallado anteriormente (ver 2.4) con el objetivo de validar que la problemática existe, así también para confirmar que las firmas sujetos de estudio no poseen la herramienta que se propone y se comprobó la disposición por parte de ellos en utilizarla para la solución de la problemática encontrada. Esto permitió recolectar información relevante que fue procesada con posterioridad.

2.6 Procesamiento de la información

Se utilizó la herramienta informática de Microsoft office Excel 2013, para la preparación de cuadros estadísticos donde se mostraron las respuestas que se obtuvieron de las encuestas y observación de la población que se sometió al proceso de investigación, en los cuales se vaciaron los datos y fueron tabulados para presentarlos en gráficos de pastel y/o de barras.

2.7 Análisis e interpretación de resultados

Se utilizaron gráficos de pastel y/o de barras, con el objeto de mostrar con mayor claridad los resultados obtenidos y así poder realizar las interpretaciones a dichos resultados.

La presentación de la información resultante de las encuestas se realizó de la siguiente manera: en primer lugar la pregunta, luego se plantea el objetivo, posteriormente se presenta el cuadro de tabulación donde se demuestra la frecuencia absoluta y relativa de los datos, en seguida se muestra el gráfico y concluyéndose con el análisis respectivo a cada pregunta. (Ver anexo 3).

2.8 Diagnóstico

La técnica que se propuso para abordar la investigación contiene dos etapas: en la primera fase la aplicación del método cualitativo, fue útil durante el acercamiento que tuvo el fin de constatar por medio de las encuestas que se entregaron a los auditores de las firmas con personería jurídica de El Salvador. En la segunda, se utilizó el cuantitativo, para analizar la información que se generó durante la recepción y captura de las encuestas que fueron contestadas por los profesionales que laboran en las entidades investigadas.

La investigación permitió conocer que la mayor parte de firmas trabajan con clientes en donde la información financiera es procesada a través del uso de TI, en tal sentido, se ha logrado obtener información relevante de como aplican la NIA 315, en lo relativo a la identificación y evaluación de riesgos de tecnología.

En seguida se presenta en forma detallada el resultado obtenido, dividido en tres subtemas importantes: influencia de la tecnología en los auditados, educación continuada y utilidad del trabajo propuesto, los cuales se desarrollan a continuación:

Influencia de las TI en los auditados

En la investigación se aprecia que un 83% de las firmas de auditoría de El Salvador que realizan actividades profesionales afirman que la información financiera, el control interno y los procesos de negocio de sus clientes dependen en algún grado de tecnologías de información y comunicación; este factor, facilitó ampliamente el cumplimiento del objetivo establecido en el instrumento seleccionado, cuyo resultado se agrupa y detalla a continuación:

Evaluación del control interno

Con respecto a la evaluación del control interno de tecnología, los auditores en la planeación incluyen algunos elementos relacionados con esta área, sin embargo se aprecia que su enfoque está basado solo en la emisión de resultados (reportes), es decir a la salida de la información; la revisión de control sobre las operaciones en los sistemas, enfocando sus esfuerzos sólo en aquellas áreas conocidas, dejando de

verificar otros aspectos importantes como el procedimiento de entrada de datos, procesamiento y seguridad del sistema. Las firmas que no lo incluyen en su estrategia de auditoría lo relacionan a la falta de personal capacitado, cuyo origen es una deficiente formación académica y falta de herramientas tecnológicas necesarias para su verificación, por lo que afirman se hace necesario el uso de un experto para evaluar dichos aspectos.

Evaluación de riesgos de TI

Es de esperarse que la aplicación de la evaluación de riesgos en la planeación de auditoría, sea un porcentaje similar, parecido o no muy alejado de los resultados de la dependencia de la informática en las empresas, sin embargo y con base a la investigación de campo, solo una de cada tres firmas utiliza con frecuencia la consideración de riesgos de tecnología de información y comunicación en la planeación de auditoría; estas los realizan mediante metodologías generales como COSO, COSO-ERM, las demás utilizan el conocimiento establecido en COBIT.

Educación continuada en las firmas de auditoría.

Las horas acreditadas de educación continuada que ostentan las firmas de auditoría, presentan una escasa intensidad en el área informática, esto trae como consecuencia dos aspectos importantes en el quehacer de los profesionales. En primer orden, la mayoría no cumplen con los requerimientos técnicos establecidos en IEPS 2, esto se debe a que no conocen el contenido de la normativa y en cierto modo, no tienen las herramientas necesarias, educación superior desactualizada, entre otros. En segundo orden, hace que la mayor parte de profesionales no utilicen técnicas de auditoría asistidas por computadora y por tanto, carecen de limitaciones sistemáticas para la identificación y evaluación de riesgos TI. Sin embargo, cabe destacar que existe en el país un grupo reducido que hacen uso de estas técnicas, las cuales se enfocan en software especializado para el análisis de pistas de auditoría, tales como IDEA, ACL, WINAUDIT, NET SCAN, AS/2 **"**AUDIT SISTEMS" y CAME AUDITORÍA.

Utilidad del trabajo propuesto.

Como parte del proceso de evaluación de control interno que las firmas realizan a las TI relevantes a la información financiera de sus clientes, la misma investigación de campo establece que más del 50% de los auditores tienen mayores riesgos en la mala aplicación de políticas contables e integridad de los datos como posibles indicios de fraudes, esto se debe a que en la actualidad los usuarios se adaptan a los sistemas y no lo contrario.

Sólo 1 de cada 10 firmas considera indispensable los conocimientos de informática que muestra su personal, esto se debe a que al desarrollar evaluaciones a la tecnología de sus clientes hacen uso de un experto, impidiendo el desarrollo de competencias exigidas por la normativa técnica aplicable. Asimismo, 7 de cada 10 firmas aclaran que en la actualidad el material es insuficiente para identificar y evaluar riesgos de TI, por consiguiente el 97% considera necesario y útil una metodología que les oriente en la ejecución de auditorías a la información financiera bajo un ambiente de sistemas computarizados, ya que al considerar dicha evaluación en sus encargos se han visto en la necesidad de que al no contar con un instrumento básico les dificulta realizar su trabajo aplicado a normas.

CAPITULO III: DESARROLLO DEL CASO PRÁCTICO

3.1 Planteamiento del caso práctico.

Introducción al estudio de caso

El presente caso práctico ha sido elaborado con el propósito de aplicar en el ejercicio profesional de los auditores, la metodología para la identificación y evaluación de riesgos TI relevantes a la información financiera. En él se presentan datos relevantes de la compañía, Recarga Directa, S.A. de C.V., la cual opera principalmente con recursos informáticos en sus actividades ordinarias. Los siguientes apartados exponen comentarios sobre el estudio del caso para ejemplificar los hechos de la práctica.

Recarga Directa, S.A. de C.V.

Recarga Directa es una compañía salvadoreña dedicada a la compra venta de planes de voz y datos, teniendo una imagen aceptable en el mercado. Ésta inició operaciones el año 1996, ha venido evolucionando su forma de comercializar, actualmente trabaja con las empresas de telefonía TIGO, DIGICEL, CLARO, TELEFONICA.

Tendencias de la industria

La industria de las telecomunicaciones por medio de celulares está en constante aumento y se debe a:

- Costo relativamente barato de los dispositivos móviles
- Facilidades de contratación del servicio pre pago
- Cobertura nacional

Esto permite que numerosas empresas se constituyan como intermediarios entre las empresas telefónicas y el consumidor final. Además, las estrategias de mercadeo impulsan el ambiente de intercomunicación móvil entre sus diferentes modalidades: línea móvil, internet.

Gobierno

La entidad formada en 1996 es gobernada a través de la junta general de accionistas, la cual establece las metas estratégicas en forma anual. Los miembros tienen domicilio en el extranjero, de nacionalidad guatemalteca y se dedican exclusivamente a la inversión en dos sociedades en particular.

Generalmente la junta requiere de los gerentes de un plan estratégico, el cual puede oscilar entre los 2 y 3 años, para el monitoreo del nivel de cumplimiento, éstos envían en forma mensual durante los primeros 6

días hábiles de cada mes, los resultados económicos y la situación financiera de la empresa. En tal información, la junta evalúa aspectos como el rendimiento, liquidez, apalancamiento financiero, entre otros.

Asimismo, de forma anual ellos evalúan los índices de clima organizacional entre los empleados de la entidad, la cual es realizada a través de encuestas y en forma confidencial. Establecen una cultura de servicio al cliente, denominada “rab il”, el cual consiste en dar un tratamiento preferencial tanto al cliente interno como al externo. Entre tanto, han inculcado los valores organizacionales, centrándose en la honestidad, orden, respeto y responsabilidad.

Empleados

Recarga Directa, S.A. de C.V. cuenta con 25 empleados a su servicio, los que están subdivididos en la forma siguiente:

Gerente general

Tiene a cargo la representación legal, y es el encargado directo ante la junta general de accionistas de los resultados económicos de la compañía.

Gerente financiero

Es responsable del flujo de efectivo para los pagos de salarios, a proveedores y demás obligaciones que mantenga la empresa, asimismo de coordinar la correcta recuperación de las ventas al crédito.

Gerente de recursos humanos

Mantiene una estricta vigilancia de los puestos de trabajo, asegurándose que tengan las cualidades necesarias que las funciones exigen, asimismo, establece capacitaciones al personal en caso de que el perfil ideal es distinto del real.

Contador general

Maneja los registros contables de la entidad, prepara los estados financieros y vela por el cumplimiento de las obligaciones formales y sustantivas en términos fiscales y financieros.

Auxiliares de contabilidad

Brindan apoyo al contador general en aspectos de la contabilidad en general.

Gestores de cobros

Apoyan a la gerencia financiera en la recuperación de cartera de clientes, son los encargados de velar porque los plazos sean mantenidos según lo establecen las políticas de crédito de cada cliente

Gerente de informática

Es el encargado de coordinar las adquisiciones, modificaciones, reparaciones y eliminaciones del recurso informático de software, hardware e información que la empresa utiliza para el desarrollo de sus actividades, así también, establece una constante vigilancia a cargo de los técnicos en informática.

Técnicos en redes informáticas

Responsables de dar mantenimiento preventivo y correctivo ante los problemas comunes relacionados con el equipo informático utilizado en el negocio de la entidad, como también para fines administrativos. Apoyan en la visita de cada kiosko en caso de algún desperfecto mecánico y comunican al jefe de informática sobre las necesidades de renovación en cuestiones de hardware.

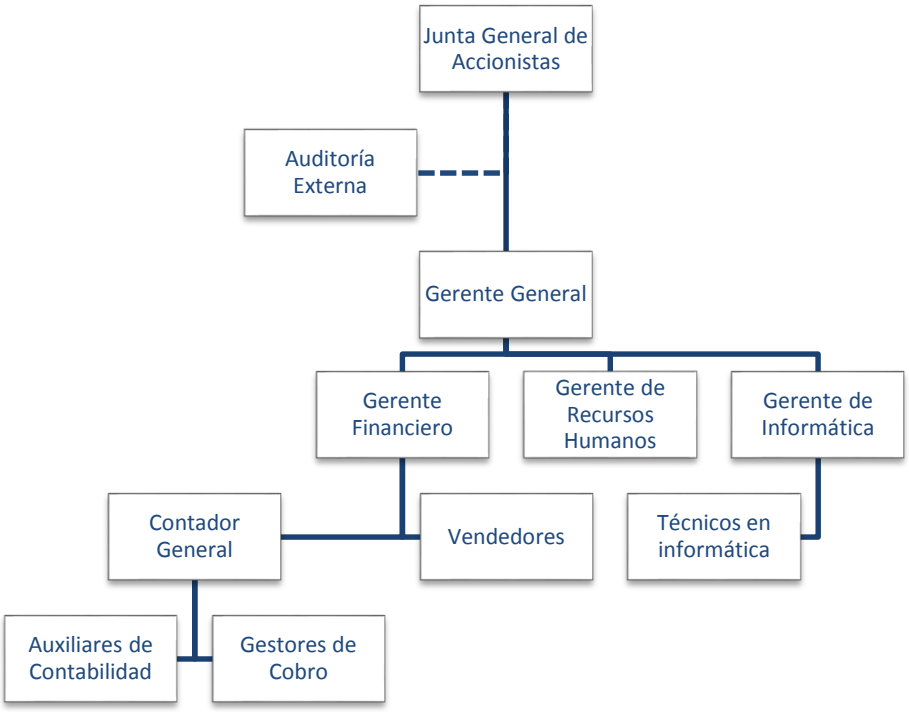
Vendedores

Personal destacado principalmente para entablar contratos con clientes para el uso y disposición de equipos POS y de Kioscos para expandir el nivel de cobertura de la compañía.

La empresa tiene la política de prohibir la contratación de personal que sean familiares entre sí, asimismo es penalizado cualquier tipo de relación sentimental que exista entre ellos.

Diagrama organizacional

Figura 2. Estructura organizativa de Recarga Directa, S.A. de C.V.



Fuente: elaboración propia.

Propiedad

La propiedad accionaria al 31 de diciembre de 2012* se describe a continuación:

Empresa	Propiedad accionaria
Recarga Directa, S.A. de C.V.	75% Inversionista "A"
	25% Inversionista "B"
Kioscos, S.A. de C.V.	75% Inversionista "A"
	25% Inversionista "B"

*Hasta la fecha la entidad no ha reportado ningún incremento/decremento en la propiedad accionaria.

Operaciones

Las principales operaciones de la empresa se caracterizan en brindar a sus clientes planes de voz y datos.

Ventas

Existen dos tipos de clientes con los cuales interactúa la entidad, los comercios afiliados y consumidores finales.

El primer grupo realiza pedidos en forma de correo electrónico o vía teléfono. Para los despachos la entidad les provee de Terminales de Punto de Venta (POS por sus siglas en inglés) los cuales son utilizados para que éstos últimos realicen recargas de saldo y/o paquetes directamente al consumidor final, de este modo cuando la empresa obtiene los pedidos hay personal encargado que los asigna los pines o códigos de las distintas denominaciones o series a cada POS, cada una de las entregas formalizadas hacia sus clientes son recibidas por medio de la tecnología Servicio General de Paquetes de Radio (GPRS por sus siglas en inglés); todas estas terminales vienen equipadas con un "tarjeta SIM" el cual lleva incorporada una cuota mensual de descarga de 3MB, la que es suficiente para recibir todos los pedidos que el cliente pueda realizar en un mes; estas tarjetas SIM son las mismas utilizadas por los teléfonos móviles, de este modo, pueden insertarse a los teléfonos y realizar navegaciones de internet hasta consumir el límite de descarga citada anteriormente.

Existen restricciones de entrega, los cuales son mayormente cuando hay falta de pago por parte del cliente, en ciertas ocasiones, se dejan de entregar los saldos debido a falta de inventario electrónico disponible. La facturación se realiza en forma inmediata al momento de la entrega del saldo/paquete, la documentación de soporte generalmente consta en el correo electrónico o el reporte que los empleados encargados de la entrega emiten para constatar la recepción de los mismos. Generalmente se cuenta con un crédito a 30 días con todos los comercios afiliados, en tal sentido, el ciclo se cierra al momento de que los documentos llegan a su vencimiento, en donde el encargado de cobros dispone del efectivo o cheques para completar la operación.

Para los clientes pertenecientes al segundo grupo la entidad ha adquirid terminales o kioskos para facilitar la venta de saldo y paquetes directamente al consumidor final. Estos utilizan también la tecnología GPRS para comunicarse directamente con el servidor y están incorporados con un "tarjeta SIM" similar al utilizado para los POS. Estos dispositivos permiten que el usuario interesado realice por cuenta propia las recargas

deseadas, mediante un novedoso y fácil sistema el cliente elige el tipo de recarga a realizar y en la cuantía requerida, el pago se hace en efectivo y éste obtiene un tiquete en sustitución de factura. La entidad maneja bolsones o cuentas de inventarios de recargas y/o paquetes de datos para cada compañía, todo consumidor final que haga uso de este sistema tiene acceso implícito al servidor en donde son resguardados todos los inventarios de saldos para teléfonos móviles. Actualmente la entidad no realiza un monitoreo constante de los movimientos que se realizan en cada kiosco, únicamente se limitan a realizar cortes semanales en los que se recoleta el efectivo depositado en cada centro de servicio. Siendo este el final del ciclo para las ventas a consumidores finales.

Recursos humanos

La gestión de los recursos humanos es realizada directamente por el gerente de recursos humanos, al no contar con asistentes es el responsable directo de realizar actividades de entrevista de aspirantes, inducción a los puestos de trabajo, comunicación de los valores organizativos, comunicación de la cultura de servicio al cliente, y de suministro del correspondiente código de ética al cual tienen todos los empleados la obligación de cumplirlo.

Nominas

Los sueldos y salarios son pagados al personal cada quince días, la empresa mantiene la política de realizar provisiones del pasivo laboral en concepto de vacaciones, aguinaldo, a excepción de las indemnizaciones que son pagadas hasta que exista obligación laboral real. Para el procesamiento de la información de planillas la empresa lo realiza mediante hojas de cálculo de EXCEL. El salario es pagado a través del Banco de América Central y es realizado mediante banca electrónica, en donde el auxiliar encargado de planillas elabora un documento en hoja de cálculo, luego es exportado hacia una página de internet establecida en forma predeterminada por el banco antes mencionado.

Compras

Para los POS la empresa realiza compras de saldos para recargas en forma semanal, las cuales son estimadas en base al consumo (ventas) realizadas en el mes inmediato anterior. De este modo, se realiza pedido directamente al proveedor por una cantidad elevada stock que se encuentra disponible hacia los clientes que deseen realizar los pedidos. Una vez que la empresa efectúa el pedido, el proveedor asigna una transferencia de series de códigos con saldo/paquetes, el cual es almacenado en servidores que para tal efecto Recarga Directa mantiene en sus instalaciones, la transferencia es realizada a través de internet.

El proveedor hace las entregas de saldo correspondiente generando así las entradas del inventario correspondiente y son custodiadas por empleados de la empresa. Las entregas son realizadas en distintas denominaciones, recargas de $1, $5, $10 y $15 y paquetes de datos de 256MB, 512MB y 1GB. Llegada la fecha de vencimiento de los documentos de compra emitido la empresa procede a pagar en forma de cheque cada una de las compras realizadas al proveedor correspondiente.

Para los kioskos, la sociedad adquiere saldo a cada proveedor de telefonía, cada compra se realiza mediante cheque y estos valores son abonados a una cuenta virtual que es manejada de forma dual entre el servidor de la empresa y la compañía telefónica, el saldo de la cuenta puede ser consultado en tiempo real y se conoce con exactitud el monto disponible para la venta.

Riesgos inherentes del negocio.

a) No existe garantía suficiente que permita asegurar que todos los despachos de saldo sean debidamente facturados al momento de realizarse, esto se debe a que la entidad no ha contemplado controles relacionados con tales entregas. Se cuenta con antecedentes que en sus inicios operativos estuvieron proporcionando recargas a sus clientes sin haberse facturado, esto afectó considerablemente los ingresos contabilizados, reconociéndose en forma incorrecta; por otra parte, el flujo de caja de la entidad tuvo serios problemas de solvencia para realizar pagos a sus proveedores y acreedores, se les pagó a 60 días plazo a pesar de que el contrato de compra establece 30 días máximo, esto ocasionó una escasez de recargas y muchos clientes se quejaron por el mal servicio, incluso se reportan que determinados clientes pasaron a la competencia. Las repercusiones no solamente son financieras, en el ámbito fiscal la entidad incumplió en este caso con la obligación formal y sustantiva de emitir los documentos de control establecidos en el código tributario, así como la del pago correspondiente del impuesto IVA y del anticipo a cuenta del impuesto sobre la renta.

b) La entidad no posee adecuadas medidas de seguridad en cuanto al manejo y custodia de los POS, estos aparatos incorporan una tarjeta SIM que fácilmente puede ser utilizado en cualquier teléfono celular capaz de navegar por internet a través de la tecnología GPRS. En este aspecto la entidad también reporta un antecedente, existió en cierta oportunidad una terminal a la cual se le sustrajo el correspondiente tarjeta SIM y el responsable tuvo acceso a navegación por internet (muy por encima de la cuota máxima establecida en el contrato 3MB), al hacerlo, la compañía que suministra el servicio de conexión no poseía con la entidad las debidas políticas límite de descarga, facilitando al agente de

este acto en la descarga de varios cientos de gigabytes de información. La entidad se negó a pagar las descargas realizadas por esta persona, argumentando que no había utilizado toda esa información para sus procesos operativos, la compañía de telecomunicación exigió pruebas contundentes que demostrasen que este último no había cometido el hecho. Al no existir pruebas irrefutables (debidas en parte a la falta de control) la entidad asumió las pérdidas económicas relativas a la descarga no autorizada realizada con la tarjeta SIM. Esto afectó en el cumplimiento de los objetivos de la entidad propuestos para el año en el que sucedió este "robo" electrónico.

c) Las ofertas promocionales que las compañías utilizan para gestionar ventas, dificultan los movimientos de inventario de recargas electrónicas. En muchas ocasiones las empresas utilizan ofertas de doble, triple, cuádruple saldo, etc. Cuando ello da lugar, la entidad procede a vender a sus clientes considerados como al consumidor final, el valor de inventario por cada dólar cobrado, es decir, que no importa el tipo de promoción del día, la entidad descarga de sus inventarios la cantidad que el consumidor final paga directamente en el momento de la operación. Según contrato, la compañía telefónica proporciona el resto de la recarga en forma directa entre esta y el consumidor final, por lo tanto, las promociones no son salidas integras del inventario manejado por la empresa Recarga Directa. La entidad actualmente no reporta ninguna irregularidad en tales transacciones, sin embargo, tampoco existen los controles adecuados que permitan asegurar que durante estas promociones el saldo completo recibido por los clientes es repartido entre la entidad y la compañía, esto pone en una seria consideración acerca de si en algún momento se haya efectuado una entrega de saldo en forma indebida, lo cual influiría directamente en el valor de inventarios presentados en los estados financieros.

d) Los kioscos distribuidos a lo largo de la república funcionan en base a monedas y billetes, cuyas denominaciones son exclusivamente de $ 1.00, en este sentido, las recargas únicamente pueden realizarse por múltiplos de la unidad. La empresa recientemente se vio involucrada en problemas, debido a que en forma intencionada los clientes depositaban $0.25, el kiosco al poseer fallas en el sensor de reconocimiento para este tipo de denominación, realizó una multiplicación de 100 por cada moneda ingresada, en este sentido, por cada $ 0.25 que el cliente insertaba, se le realizaba una recarga electrónica valorado en $ 25.00, esto repercutió gravemente en los movimientos reales de inventario, también en el registro correcto de los ingresos, ya que el inventario se despachaba en forma superior a lo que lo reflejado contablemente.

A continuación se presentan los Estados Financieros del ejercicio 2012, de la compañía sujeta a estudio.

RECARGA DIRECTA, S.A. DE C.V.
Estado de situación financiera
Al 31 de diciembre de 2011 y 2012
(Cifras expresadas en US $ Dólares)

	2011	2012
ACTIVOS		
Efectivo	31,500	35,424
Deudores comerciales y otras cuentas por cobrar	405,400	450,444
Inventarios	62,100	69,210
Activos corrientes	**499,000**	**555,078**
Propiedades planta y equipo	600,384	667,709
Activos intangibles	23,216	24,546
Activos no corrientes	**623,600**	**692,255**
Activos totales	**1122,600**	**1247,333**
PASIVOS Y PATRIMONIO		
Acreedores comerciales	38,708	43,009
Impuestos corrientes por pagar	348,397	27,222
Provisión para obligaciones	108,000	25,275
Pasivos corrientes	**495,105**	**95,506**
Préstamos bancarios	167,466	269,918
Pasivos no corrientes	**167,466**	**269,918**
Pasivos totales	**662,571**	**365,424**
Capital social	250,000	250,000
Ganancias acumuladas	167,374	581,909
Reserva legal	42,656	50,000
Patrimonio	**460,029**	**881,909**
Total pasivo y patrimonio	**1122,600**	**1247,333**

Las notas son parte integrante de los estados financieros.

Representante Legal	Contador General	Auditor Externo

Estado del resultado integral y ganancias acumuladas
Del 01 de enero al 31 de diciembre de 2011 y 2012
(Cifras expresadas en US $ Dólares)

	2011	**2012**
Ingreso por venta de recargas	2281,210	2423,808
Costo de venta	-1468,905	-1598,783
Ganancia bruta	**812,305**	**825,025**
Otros ingresos	88,789	98,654
Gastos de venta	-130,588	-145,098
Gastos de administración	-88,592	-98,435
Otros gastos	-1,148	-1,276
Gastos financieros	-71,400	-79,333
Ganancia antes de impuesto y reserva	**609,366**	**599,537**
Reserva legal	-42,656	-7,344
Ganancia antes de impuesto	**566,710**	**592,193**
Impuesto sobre la renta	-141,678	-177,658
Ganancia del año	**425,033**	**414,535**
Ganancias acumuladas al inicio del año	-257,659	167,374
Dividendos	-	-
Ganancias acumuladas al final del año	167,374	581,909

Las notas son parte integrante de los estados financieros.

Representante Legal	Contador General	Auditor Externo

3.2 Descripción general de la metodología

DESCRIPCIÓN GENERAL DE LA METODOLOGÍA

ALCANCE:

En esta propuesta, se incluyen la mayoría de aspectos para la evaluación de riesgos del ambiente de TI y los controles, podrá adaptarse a las circunstancias de la empresa auditada. A partir de generar el mapa de los recursos informáticos utilizados por la entidad, se infiere a juicio del equipo de investigación, aquellos componentes que tienen impacto en los estados financieros, el auditor responsable puede utilizar su juicio profesional para determinar los casos específicos aplicables a la entidad sujeta a examen. Asimismo se omiten los aspectos generales del memorándum de planeación, como los procedimientos para obtener conocimientos básicos de la entidad auditada como clientes, proveedores, información de partes relacionadas, entre otros.

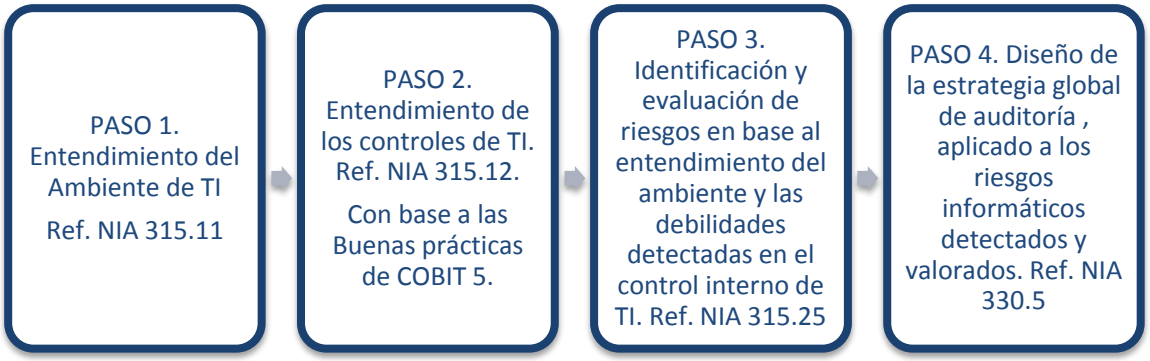
Los pasos a seguir para la solución del caso planteado contempla el supuesto que toda esta información (a excepción de los ciclos operativos) ha sido obtenida por el auditor a través de lo establecido en la NICC 1 y NIA 220, en cuanto a las políticas y procedimientos para la aceptación y la continuidad de las relaciones con clientes.

La metodología inicia con un entendimiento del ambiente de las tecnologías que maneja la empresa cliente, esto le permite al auditor conocer los recursos informáticos que utiliza la entidad y para qué son utilizados. Luego debe realizarse un estudio y evaluación del control interno de TI, únicamente a aquellos aspectos que tengan incidencia en los estados financieros. Más tarde, son identificados y evaluados cada uno de los riesgos que a juicio profesional del auditor pueden afectar las cifras expresadas en la información financiera, permitiéndole según la NIA 315, establecer un enfoque global para diseñar la oportunidad, naturaleza y extensión de los procedimientos sustantivos que ayudarán al auditor a tomar conclusiones que le servirán para su opinión.

En el ejercicio de sus actividades profesionales, el auditor puede utilizar las debilidades de control interno identificadas para comunicarlas al nivel adecuado de la empresa de acuerdo a la NIA 265, que incluyan los posibles indicios de fraudes, cartas de gerencia que expresen lo adecuado de los controles internos, entre otros.

En resumen, los pasos de la metodología para la identificación y valoración de riesgos, se exponen en la siguiente figura:

Figura 3. Proceso para identificar y valorar riesgos de TI.



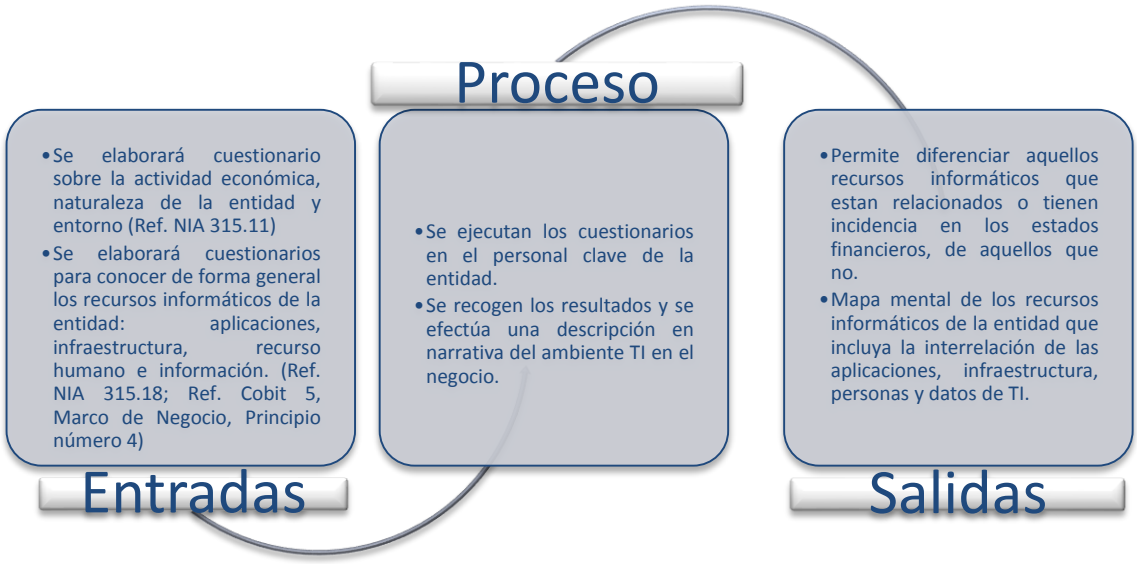
Fuente: elaboración propia.

A continuación se describe cada paso:

Paso 1.

El primer paso consiste en el entendimiento del ambiente de TI en el negocio, para ello se debe realizar lo siguiente:

Figura 4. Proceso para el entendimiento del ambiente de TI en el negocio.

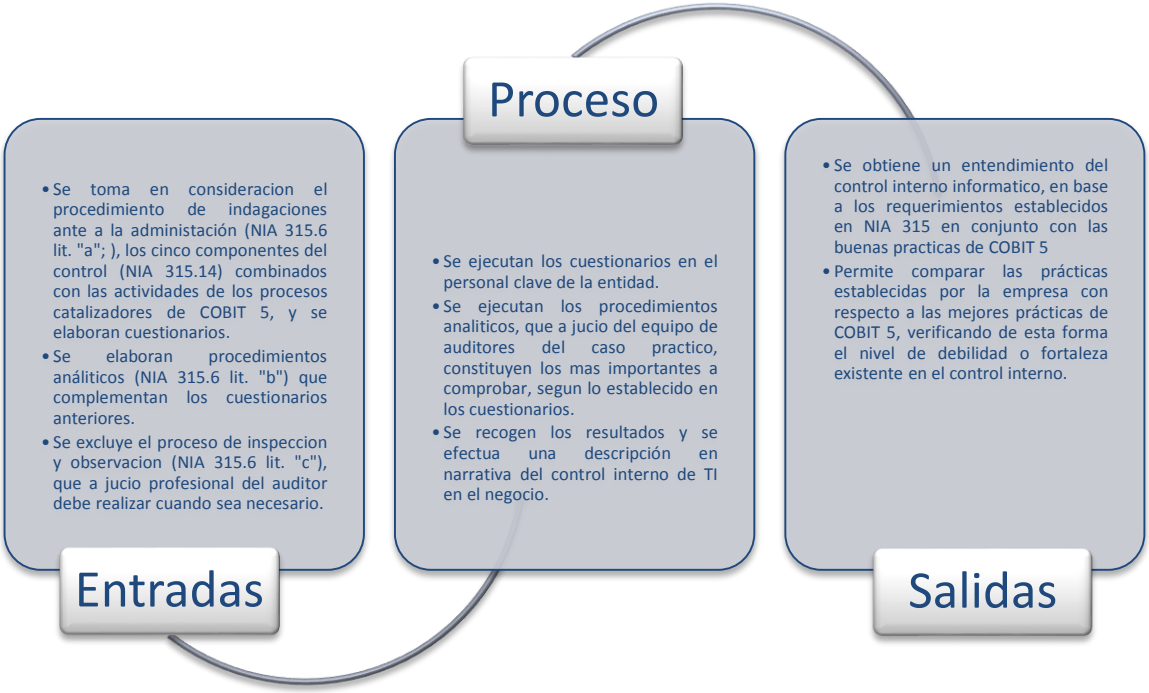


Fuente: elaboración propia.

Paso 2.

El segundo paso se trata de comprender el control interno y su entorno. Este entendimiento debe ser un proceso continuo, dinámico, de obtener, actualizar y analizar información a través de la auditoría. Se trata de comprender el control interno establecido por la entidad hacia la TI relevante a los estados financieros, se deja de lado por tanto aquellos aspectos informáticos que no poseen incidencia y se enfoca el estudio en base a los principios y buenas practicas del marco de COBIT 5, así:

Figura 5. Proceso para la comprensión del control interno y su entorno.



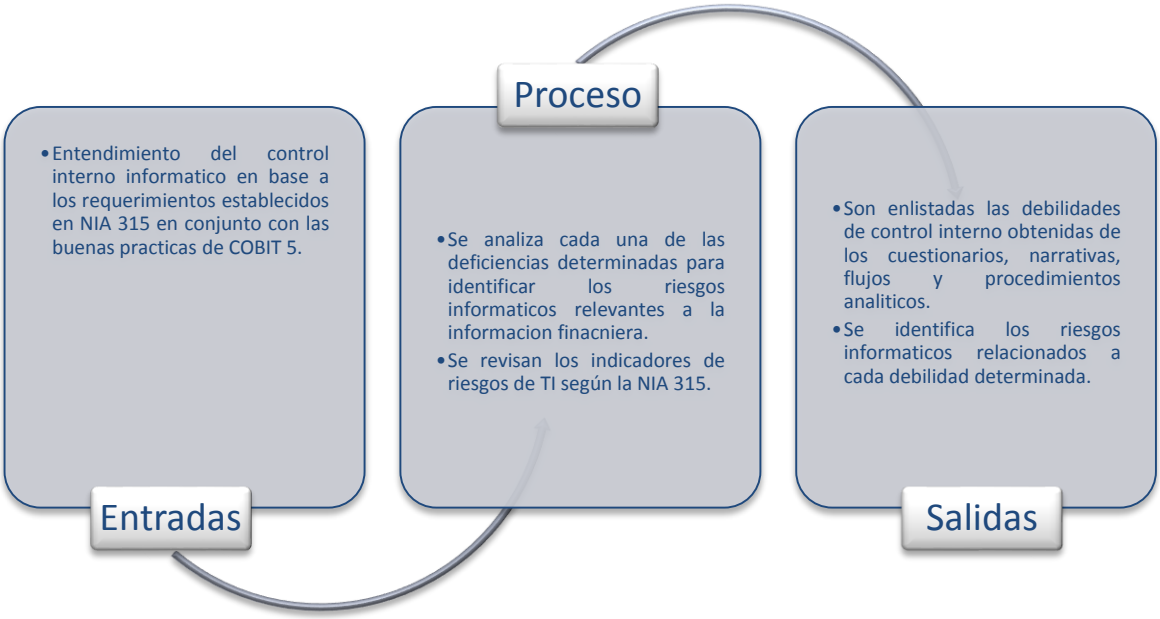
Fuente: elaboración propia.

Después de comparar las buenas prácticas de COBIT 5, el auditor financiero tendrá un marco, listado o detalle de los principales incumplimientos de la entidad, es decir, en el entendido que cubran e identifiquen los riesgos posibles de TI a nivel de empresa y de controles, los indicadores encontrados corresponderán a aquellos que requieren principal atención del auditor.

Paso 3.

El tercer paso consiste en identificar aquellos riesgos de TI relevantes a la auditoría de estados financieros, para lograrlo se procede de la siguiente manera:

Figura 6. Proceso para identificar riesgos de TI relevante a la información financiera.

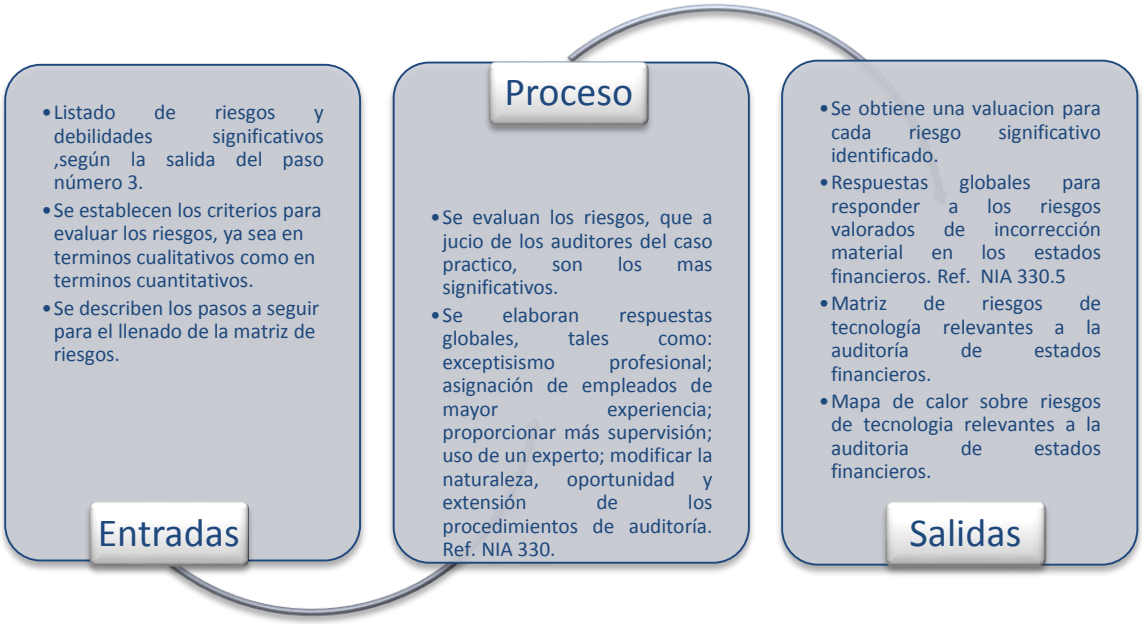


Fuente: elaboración propia.

Paso 4.

El cuarto paso consiste en desarrollar un enfoque global del alcance de la naturaleza, oportunidad y extensión de los procedimientos de auditoría, por medio de la valoración de riesgos identificados en el paso anterior, de la confección de una matriz y un mapa de calor.

Figura 7. Diseño del enfoque global (naturaleza, oportunidad y extensión) de los procedimientos de auditoría.



Fuente: elaboración propia.

3.3 Solución del caso práctico (aplicación de la metodología en cuatro pasos)

3.3.1 Paso 1: entendimiento de naturaleza de las TI en la empresa

Con base a la descripción general de la metodología (paso 1), se procede a identificar el ambiente de TI que posee la entidad por medio del siguiente cuestionario:

Tabla 4. Entendimiento de naturaleza de las TI en la empresa.

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE:	PERIODO	REF.
RECARGA DIRECTA, S.A. DE C.V.	2012	

OBJETIVO:

Obtener entendimiento suficiente y adecuado, sobre el uso de la tecnología de información en la entidad, indagando sobre: infraestructura, aplicaciones, personas y datos; así como también los ciclos de ventas, compras y principales riesgos inherentes.

PROCEDIMIENTOS:

Ejecute el siguiente cuestionario de conocimiento del ambiente de TI mediante indagaciones ante la administración, de ser necesario realice comprobaciones de observación e inspección incluyendo procedimientos analíticos, como sustento a las respuestas de la entidad.

1	ENTENDIMIENTO DE NATURALEZA DE LAS TI EN LA EMPRESA	SI	NO	N/A	COMENTARIO	REF. COBIT 5	REF. NIA
1.1	**NATURALEZA DE LA ENTIDAD** Se identifican los datos generales del cliente, incluyendo el giro o la actividad principal a la que se dedica la empresa, sus relaciones con otras entidades, etc. - ¿Realiza la entidad transacciones de comercio electrónico B2B, B2C, entre otros? - ¿Posee la entidad un ambiente de microcomputadoras independientes?	X X					NIA 315.11

	- ¿Posee la entidad un ambiente de computadoras interconectados?	X					
1.2	**RECURSOS INFORMÁTICOS**						
1.2.1	**SOFTWARE** ¿Cuáles son las principales aplicaciones que la empresa dispone para su uso, sean estos propios o de terceros?				Disponemos de aplicaciones instaladas en los kioscos "POSMOBILE", el sistema operativo de cada terminal y el sistema operativo del servidor. Para la contabilidad y administración utilizamos el ASPEL COI 6.0, ASPEL SAE 5.0		NIA 315. Anexo 1.5
1.2.2	**INFRAESTRUCTURA** Cuál es la infraestructura física que posee la empresa, sean propios o de terceros para la operación y el funcionamiento del sistema o sistemas relacionados con la actividad del negocio, en general detalle: servidores, estaciones de trabajo, cableado y estructurado de red física e inalámbrica, equipo de protección o seguridad, entre otros.				Poseemos 3 servidores, uno para administrar las recargas de saldo y otro para las recargas de datos, el ultimo es para uso interno. 100 kioscos o puntos de venta a lo largo de todo el país. 150 POS o puntos de venta a lo largo del país, Los kioskos y POS se conectan mediante tarjeta SIM con tecnología GPRS.		NIA 315.6b , A7
1.2.3	**PERSONAS** Liste las personas involucradas en el ambiente de TI, el auditor financiero conocerá de las personas involucradas en la gestión, administración, operación y				La empresa cuenta con: Un gerente de informática(administrador)		NIA 315. Anexo 1.5

	mantenimiento del sistema. De la misma forma detalle los principales usuarios del Sistema o software contable.				15 técnicos para darle soporte a los kioscos y a los POS. Los principales usuarios del sistema administrativo y contable son: El gerente financiero. El contador general. Los auxiliares contables.		
1.2.4	**DATOS** Liste los sistemas, software o aplicaciones del sistema de información empresarial que participan en el registro, proceso y salida de la información.				La información de los sistemas de puntos de venta se maneja en base de datos SQL SERVER 2010. La información financiera contable y administrativa está en base de datos FIREBIRD 2.5.		NIA 315. Anexo 1.5
1.3	De la información anterior, elabore un mapa o estructura que identifique claramente los recursos informáticos de la entidad						

EVIDENCIA DE REVISIÓN:

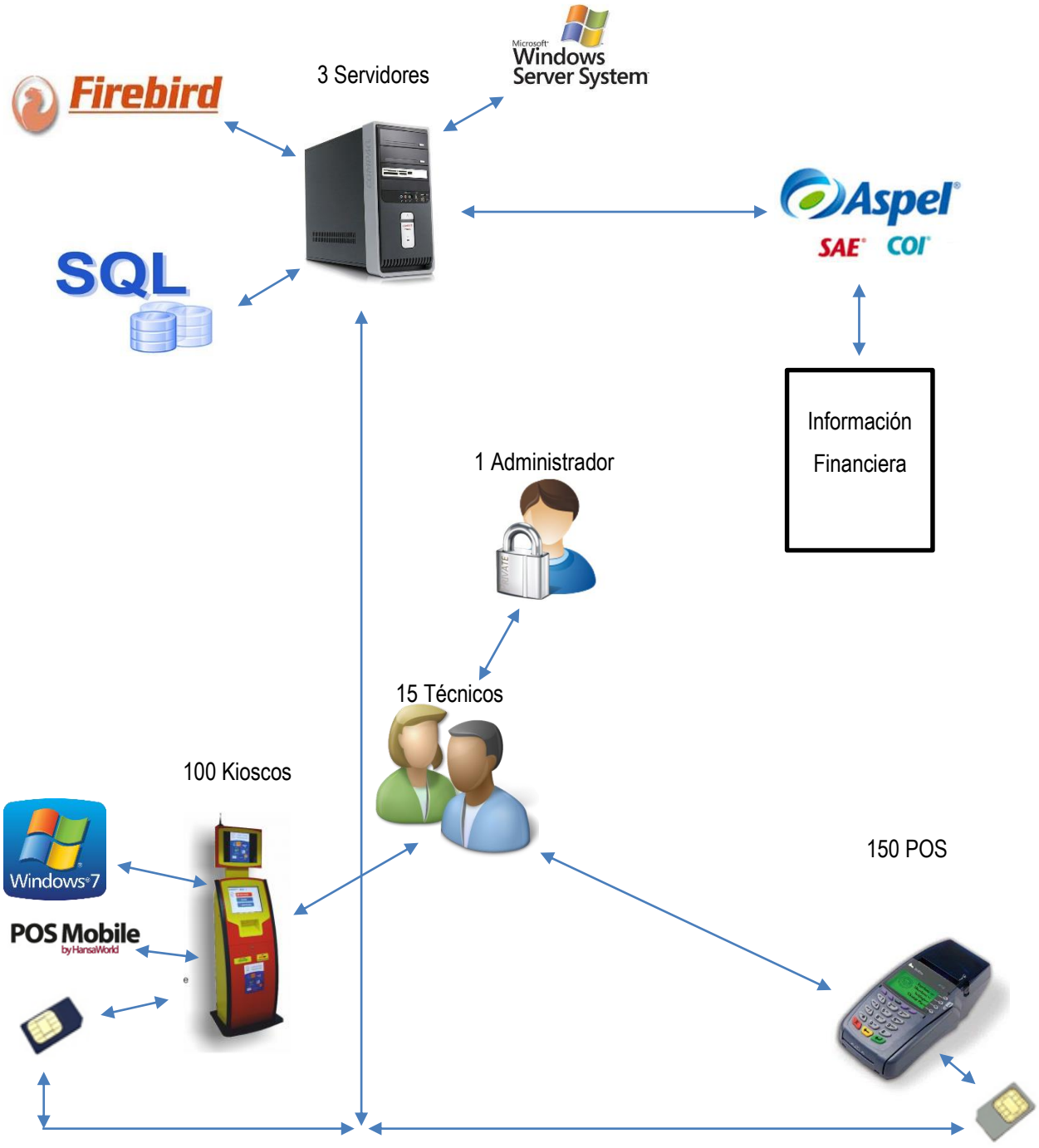
	NOMBRE	**FECHA**	**FIRMA**
ELABORÓ	**Manuel Antonio Guardado Quintanilla**	**05/11/13**	
REVISÓ	**Oscar Alcides Montiel Hernández**	**05/11/13**	
AUTORIZÓ	**Ludwig Javier Guzmán Sosa**	**05/11/13**	

Fuente: elaboración propia.

De las respuestas extraídas en el presente cuestionario, los auditores del caso práctico obtienen información importante relacionada con los recursos informáticos que maneja la entidad, sean estos de infraestructura, personas, datos y aplicaciones.

Como parte de las salidas establecidas en la metodología, se presenta a continuación el mapa mental de las tecnologías de información y la forma en cómo interactúan entre sí:

Figura 8. Mapa mental de los recursos informáticos de la entidad.



Fuente: elaboración propia.

Explicación del mapa mental: el gerente de informática tiene a cargo 15 técnicos destinados para dar soporte y mantenimiento a todos los POS y kioscos distribuidos a lo largo del país, los kioscos poseen sistema operativo Windows 7 y llevan instalado el software POS MOBILE, el cual sirve de interfaz entre el consumidor y las recargas, los POS son utilizados en cada comercio afiliado y vienen equipados – al igual que los kioscos – de tarjetas SIM. Estas tarjetas sirven para comunicarse directamente con cada uno de los tres servidores establecidos para tal efecto. Esta información trasmitida es procesada en bases de datos SQL y FIREBIRD, cada uno de los servidores poseen el sistema operativo Windows Server 2010. Al procesar la información se realiza una migración manual de las transacciones de recargas hacia el sistema ASPEL (SAE y COI), el cual clasifica, resume y prepara la información establecida en los estados financieros.

3.3.2 Paso 2: entendimiento del control interno de tecnología de información.

Una vez conocidos los recursos informáticos con que cuenta Recarga Directa, S.A. de C.V., es momento que los auditores identifiquen y evalúen los riesgos informáticos a los que se expone la entidad, pero antes es necesario obtener un entendimiento de cada uno de los controles internos que se han establecido en dichos activos. Para tal entendimiento el equipo deberá cumplir el proceso descrito en la NIA 315 párrafos 7, el cual establece la obligación de ejecutar ciertos procedimientos que en el presente caso práctico han sido adoptados de la siguiente manera:

a) Indagaciones con la administración NIA 315, párrafo 7, literal a)

Están descritos a través de tablas que muestran los cinco componentes del control interno, en base a la NIA 315 relacionada en conjunto con las buenas prácticas de COBIT 5. Tales componentes se detallan a continuación:

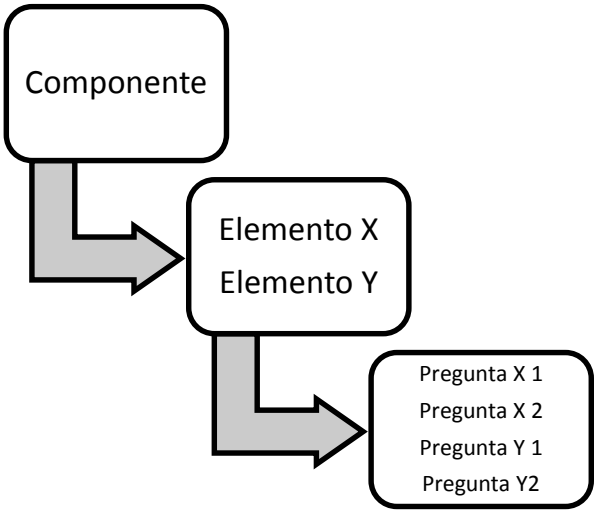
- ✓ Entorno de control
- ✓ Proceso de valoración de riesgo
- ✓ Sistema de información y comunicación
- ✓ Actividad de control
- ✓ Seguimiento de controles

Cada cuestionario conlleva una serie de preguntas que son clasificados por el equipo de trabajo por elementos, y a su vez, son agrupados en cada uno de los componentes citados. Esto se hace con el

propósito de poder crear un efecto cascada que facilita el trabajo del auditor en la implementación de esta metodología.

La descripción grafica del efecto cascada propuesta en el presente documento queda establecido de la siguiente manera:

Figura 9. Estructura del cuestionario de evaluación del control interno



Fuente: elaboración propia.

Cada uno de los componentes del control interno lleva incorporada una serie de elementos que describen específicamente el área de informática al cual pertenece, de igual modo, cada elemento está compuesto por preguntas que permiten al auditor conocer el control interno TI.

Estas preguntas han sido extraídas por el equipo de trabajo de las actividades plasmadas en COBIT 5, cada una de estas representan las buenas prácticas que las empresas deben realizar con el propósito que su control interno informático sea robusto. Por tanto, en la medida que las preguntas vayan generando respuestas negativas, será un indicador de una debilidad del control, por el contrario, una respuesta afirmativa implica una fortaleza del control.

b) Observación e inspección

Queda expresado implícitamente, es decir, no se incluye en el presente caso aquellas comprobaciones visuales que deba realizar el auditor, ya que tales serán valorados en la práctica según el juicio profesional.

c) Procedimientos analíticos

Son incluidos como un complemento útil de los cuestionarios, tienen como finalidad proveer al auditor de valiosos conocimientos técnicos-informáticos para la evaluación de los riesgos. Cabe mencionar que estos procedimientos son distintos a los tradicionales (cálculo de coeficientes, tendencias, porcentajes, etc.). De este modo, para un adecuado análisis de las vulnerabilidades TI se propone realizar actividades tales como:

- Verificar las cantidades de usuario con perfil “Administrador”, o con denominaciones incompatibles con las políticas de seguridad informática, por ejemplo usuarios “Prueba”.
- Comprobar la realización de registros contables sin autorización o en periodos cerrados.
- Probar cambios no autorizados en valores parametrizables (porcentajes de depreciación, amortización, impuestos e importes de estimación incobrables, entre otros).
- Revisar de la bitácora del sistema, con especial énfasis a aquellas transacciones realizadas en horarios extra-laborales, su posible modificación por parte del “Administrador”.

Estos procedimientos analíticos son realizados en función del grado de importancia, considerándose como de carácter instructivo al momento del análisis del riesgo informático. Tales actividades son incluidas en el anexo 8. En resumen, para la evaluación del riesgo del enunciado se ha procedido en la siguiente forma:

Figura 10. Procedimientos de evaluación de riesgo.

Fuente: IFAC, NIA 315, "Identificación y valoración de los riesgos de incorrección material mediante el conocimiento de la entidad y de su entorno”, 2011, párrafo 7.

Dicho lo anterior, el paso 2 comprende las indagaciones con la administración para cada componente del control interno, como se expone a continuación:

1) **Componente: entorno de control**

Objetivo: conocer los puntos fuertes de los elementos del entorno de control que permitan proporcionar una base adecuada para los demás componentes del control interno TI

La tabla siguiente muestra un resumen de los objetivos por cada elemento considerado en el cuestionario de 133 preguntas para verificación del entorno de control.

Tabla 5. Objetivos del componente entorno de control.

No.	ELEMENTO	COBIT 5	NIA	OBJETIVO
1.1	**La comunicación**			
1.1.1	**Evaluación de los requisitos para elaborar informes a las partes interesadas (accionistas, proveedores, auditores)**	EDM05.01	NIA 315.A69 y A70 literal a)	Conocer si la entidad cuenta con principios de comunicación, tales como los formatos sugeridos y canales de comunicación con los distintos usuarios de la información financiera (interna y externa).
1.1.2	**Orientación de la comunicación con las partes interesadas y para la elaboración de informes**	EDM05.02	NIA 315.A69 y A70 literal a)	Indagar sobre la existencia de una estrategia de comunicación, por parte de la entidad hacia las partes interesadas (internas y externas) de la información, que garantice el cumplimiento de los requisitos corporativos y los mecanismos de validación, aprobación de informes con el fin de asegurar la calidad y completitud de la información.
1.1.3	**Supervisión de la comunicación con las partes interesadas**	EDM05.03	NIA 315.A69 y A70 literal a)	Obtener conocimiento sobre si la entidad realiza evaluaciones a los mecanismos de comunicación que aseguren la precisión y fiabilidad, así como el cumplimiento a los requisitos de los diferentes interesados de la información.
1.1.4	**Comunicar los objetivos y la dirección de gestión**	APO01.04	NIA 315.A69 y A70 literal a)	Determinar si existe una adecuada comunicación y comprensión de los objetivos y la dirección del departamento de TI, así como también si dichas comunicaciones reciben el

No.	ELEMENTO	COBIT 5	NIA	OBJETIVO
				apoyo de la dirección ejecutiva en los diferentes niveles jerárquicos de la entidad, si están alineados con la misión de la empresa y si los recursos son suficientes para el soporte del proceso de comunicación.
1.1.5	**Comunicar la estrategia y la dirección de ti**	APO02.06	NIA 315.A69 y A70 literal a)	Conocer si la entidad cuenta con procesos que apoyen y aprueben la estrategia que tienen las TI dentro de la misma. Asimismo, si se ha desarrollado un plan en el que se definan los mensajes, canales, horarios y a quienes comunicar.
1.2	**Compromiso por la competencia**			
1.2.1	**Mantener las habilidades y competencias del personal**	APO07.03	NIA 315.A70 literal g)	Identificar como es la cultura de las habilidades y competencias del personal dentro de la entidad, para comprender si tales habilidades y competencias se encuentran al nivel requerido, para cumplir con las metas empresariales y el grado de dependencia que pudiese existir de personas claves en la empresa.
1.2.2	**Evaluar el desempeño laboral de los empleados**	APO07.04	NIA 315.A70 literal g)	Verificar la existencia sobre programas para evaluar la competencia del personal, y si este incluye metas individuales por puestos alineadas a los objetivos trazados por la entidad, recompensa a logros alcanzados y que el proceso se aplique de forma coherente y en concordancia con las políticas de la organización.
1.3	**Participación de los responsables del gobierno de la entidad**			
1.3.1	**Evaluación del sistema de gobierno**	EDM01.01	NIA 315.A70 literal c)	Indagar sobre la existencia y ejecución de políticas sobre la función que posee la gerencia de TI en referencia al control interno global de la entidad.

No.	ELEMENTO	COBIT 5	NIA	OBJETIVO
1.4	**Orientación del sistema de gobierno.**	EDM01.02	NIA 315.A70 literal c)	Conocer sobre los aspectos relacionados a los principios del gobierno de TI y los cuales se encuentren alineados a las estructura organizativa y los procesos de negocios de la entidad.
1.5	**Supervisión del sistema de gobierno**	EDM01.03	NIA 315.A70 literal c)	Comprender que la entidad cuenta con una supervisión adecuada para dar cumplimiento a los principios adoptados por el gobierno de TI, en cuanto a la efectividad y rendimiento hacia el negocio.
1.6	**El apetito por el riesgo o filosofía para la gestión del riesgo**			
1.6.1	**Evaluación de la gestión de riesgos**	EDM03.01	NIA 315.A70 literal d)	Indagar sobre la filosofía de riesgos informáticos que ha establecido la entidad y pudiesen afectar los riesgos de negocio, así como el establecimiento de niveles para poder asumir o rechazar algún riesgo u oportunidad y que las medidas a tomar se encuentren alineadas con los objetivos organizacionales.
1.7	**Orientación de la gestión de los riesgos**	EDM03.02	NIA 315.A70 literal d)	Conocer del nivel de promoción que hace la entidad de la cultura de riesgos de TI entre su personal, con el fin de determinar el compromiso y comunicación que se tiene ante un riesgo u oportunidad identificado en las operaciones de la empresa.
1.8	**Supervisión de la gestión de riesgos**	EDM03.03	NIA 315.A70 literal d)	Indagar sobre la existencia de políticas y procedimientos en el desarrollo de la supervisión, en la gestión de los riesgos, que sean conformes a los umbrales del apetito del riesgo considerados por la entidad.
1.9	**Estructura organizativa**			

No.	ELEMENTO	COBIT 5	NIA	OBJETIVO
1.9.1	**Definir la estructura organizativa**	APO01.01	NIA 315.A70 literal e)	Determinar los distintos niveles jerárquicos y la independencia que se posee dentro de la estructura organizativa en los cuales se planifica, ejecuta, controlan y revisan las actividades de la entidad, que requieren en cierta medida de procesos automatizados para alcanzar sus objetivos.
1.9.2	**Optimizar la ubicación de la función de ti**	APO01.05	NIA 315.A70 literal e)	Conocer la importancia de la función de TI en la entidad según el grado de dependencia dentro de la organización.
1.10	**Recursos humanos**			
1.10.1	**Mantener suficiente y adecuado la dotación de personal**	APO07.01	NIA 315.A70 literal g)	Indagar si la entidad evalúa las necesidades de personal en forma regular o en cambios importantes en la empresa, operativos o en los entornos para asegurar que se tienen suficientes recursos humanos para apoyar las metas y objetivos empresariales.
1.10.2	**Identificar personal clave de ti.**	APO07.02	NIA 315.A70 literal g)	Identificar la existencia de personal clave de TI, con el fin de determinar la dependencia que pudiese existir en el departamento informático y como planifica la sucesión para este tipo de personas.
1.10.3	**Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio**	APO07.05	NIA 315.A70 literal g)	Conocer las políticas y procedimientos que aplica la entidad para entender la demanda actual y futura de personal en apoyo al logro de los objetivos de negocio y de TI.
1.10.4	**Gestionar el personal contratado**	APO07.06	NIA 315.A70 literal g)	Indagar sobre la existencia y aplicabilidad de procedimientos para contratación de personal, con el fin de que se reclute a aquellos con las competencias y habilidades requeridas a la función a desempeñar.
1.10.5	**Información confidencial**			Conocer si la entidad mantiene información confidencial y de ser así, que políticas posee para garantizar que

No.	ELEMENTO	COBIT 5	NIA	OBJETIVO
				dicha información no sea extraída por los empleados para otros fines.

Fuente: elaboración propia.

Tabla 6. Cuestionario del componente entorno de control.

CLIENTE:	PERIODO	REF.
RECARGA DIRECTA, S.A. DE C.V.	2012	

OBJETIVO:

Obtener entendimiento suficiente y adecuado sobre los riesgos de TI en la empresa, mediante la evaluación del control interno de la entidad, conforme a los componentes: ambiente de control; proceso de valoración del riesgo por parte de la entidad; sistemas de información comunicación; actividades de control y seguimiento de los controles. Ref. NIA 315.14 y COBIT.

PROCEDIMIENTOS:

Ejecute el siguiente cuestionario de conocimiento de los controles de TI mediante indagaciones ante la administración, de ser necesario realice comprobaciones de observación e inspección incluyendo procedimientos analíticos, como sustento a las respuestas de la entidad.

1	ENTORNO DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	Objetivo: conocer los puntos fuertes de los elementos del entorno de control que permitan proporcionar una base adecuada para los demás componentes del control interno TI.					
1.1	**La comunicación**					
1.1.1	**Evaluación de los requisitos para elaborar informes a las partes interesadas (accionistas, proveedores, auditores)**				**EDM05.01**	NIA 315.A69 y A70 literal a)

1	ENTORNO DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	¿La empresa cuenta con principios de comunicación que especifiquen los formatos para comunicar?	X				
	¿La empresa cuenta con principios de comunicación que especifiquen los canales para comunicar?	X				
1.1.2	**Orientación de la comunicación con las partes interesadas y para la elaboración de informes**				**EDM05.02**	NIA 315.A69 y A70 literal a)
	¿La empresa posee una estrategia de comunicación hacia las partes interesadas TI externas e internas?	X				
	¿La empresa utiliza mecanismos que garanticen que las comunicaciones cumplen con los requisitos corporativos obligatorios?	X				
	Al momento de comunicar un mensaje ¿Existe un mecanismo para validar y aprobar la información comunicada?	X				
1.1.3	**Supervisión de la comunicación con las partes interesadas**				**EDM05.03**	NIA 315.A69 literal a)
	¿La empresa evalúa periódicamente la eficacia de los mecanismos para asegurar la precisión y fiabilidad de la información comunicada?	X				
	¿La empresa determina si los requisitos de los diferentes interesados se están cumpliendo?	X				
1.1.4	**Comunicar los objetivos y la dirección de gestión**				**APO01.04**	NIA 315.A69 y A70 literal a)
	¿La empresa comunica continuamente los objetivos y la dirección establecida del departamento de informática?	X				
	¿Las comunicaciones reciben el apoyo del gerente general?	X				
	¿La información que es comunicada toma en consideración la misión de la empresa y los objetivos del servicio de TI?	X				
	¿La información que es comunicada toma en cuenta la calidad, claridad y comprensión del mensaje?	X				

1	ENTORNO DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	¿Existen recursos suficientes para dar soporte al proceso de comunicación, canales de comunicación por ejemplo, correo interno?	X				
1.1.5	**Comunicar la estrategia y la dirección de ti**				**APO02.06**	NIA 315.A69 literal a)
	¿La empresa ha establecido un proceso para apoyar y aprobar la estrategia del departamento de informática?	X				
	¿La empresa ha desarrollado un plan de comunicación que cubra los mensajes necesarios, la audiencia objetivo, los canales de comunicación y los horarios de comunicación?	X				
	¿Es actualizado según sea necesario el plan de comunicación y estrategia?	X				
1.2	**Compromiso por la competencia**					
1.2.1	**Mantener las habilidades y competencias del personal**				**APO07.03**	NIA 315.A70 literal g)
	¿Están definidos las habilidades necesarias del personal para lograr los objetivos del departamento informático y procesos de TI?	X				
	¿La entidad cuenta con una planificación formal para fomentar el desarrollo de competencias, oportunidades de progreso personal?	X				
	¿La entidad cuenta con una planificación formal de la carrera profesional para fomentar una menor dependencia de personal clave?		X			
	¿La entidad lleva a cabo revisiones periódicas para evaluar la planificación de la sucesión?		X			
	¿La entidad proporciona repositorios de conocimiento para apoyar el desarrollo de competencias en el personal de informática?	X				
	¿La empresa ha identificado las diferencias existentes entre las habilidades necesarias y las disponibles del personal de informática?	X				

1	ENTORNO DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	¿La empresa ha desarrollado programas de formación al personal de informática?	X				
	¿Estos programas incluyen conocimiento de la empresa, control interno de TI?		X			
	¿La entidad lleva a cabo revisiones periódicas para evaluar las habilidades del personal informático?	X				
	¿Los programas de formación son revisados para asegurarse que están cumpliendo con las necesidades de conocimientos, aptitudes y habilidades?	X				
1.2.2	**Evaluar el desempeño laboral de los empleados**				**APO07.04**	NIA 315.A70 literal g)
	Al momento de establecer las metas individuales del personal informático ¿Se consideran los objetivos funcionales del departamento de informática?	X				
	¿Las metas están basadas en objetivos SMART (específicos, medibles, realizables, pertinentes)?	X				
	¿Las metas reflejan las competencias básicas del personal TI, los valores empresariales?	X				
	¿Se realizan evaluaciones de desempeño de 360 grados en el personal de informática, es decir evaluaciones cruzadas entre los distintos tipos de jerarquía organizacional?	X				
	¿Se ha implementado un proceso disciplinario al personal TI?	X				
	¿Existen instrucciones específicas para el uso de la información personal obtenida del proceso de evaluación?	X				
	¿Las instrucciones se encuentran elaborados según legislación laboral vigente?			X		
	¿Se proporciona retroalimentación oportuna sobre el desempeño frente a las metas del individuo?	X				

1	ENTORNO DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	¿Existe un proceso de remuneración y/o reconocimiento que premie el desarrollo de competencias?	X				
	¿Existe un proceso de remuneración y/o reconocimiento que premie el logro de los objetivos del departamento de TI?	X				
	¿Se han desarrollado planes de mejora del desempeño basados en los resultados del proceso de evaluación?	X				
1.3	**Participación de los responsables del gobierno de la entidad**					
1.3.1	**Evaluación del sistema de gobierno**				**EDM01.01**	NIA 315.A70 literal c)
	¿En el diseño de las funciones de gerencia TI se considera el control interno del resto de la empresa?	X				
	¿Están debidamente analizadas las obligaciones legales del gerente TI para con la empresa, por ejemplo conocimiento del código fuente de los programas, secretos empresariales?	X				
	¿Se ha determinado la relevancia de TI y su papel con respecto al negocio?	X				
	¿La empresa cuenta con pasos que guían el diseño de la toma de decisiones del Gerente TI?	X				
	¿El Gerente TI comprende la cultura empresarial de la toma de decisiones?	X				
	¿El Gerente de TI ha determinado los niveles apropiados para delegar autoridad a los técnicos en informática?	X				
1.4	**Orientación del sistema de gobierno.**				**EDM01.02**	NIA 315.A70 literal c)
	¿Se han comunicado los principios por el cual se desenvuelve el Gerente de TI?	X				
	¿El Gerente de TI ha establecido un liderazgo informado y comprometido?	X				
	¿Los principios del Gerente de TI se encuentran alineados con la estructura	X				

1	ENTORNO DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	organizativa y con los procesos de gerencia general?					
	¿Los principios del Gerente de TI se encuentran alineados con los procesos y prácticas de la gerencia general?	X				
	¿Los mecanismos de comunicación proporcionan información adecuada a los responsables de la supervisión y toma de decisiones?	X				
	¿El personal de informática ha sido instruido para que demuestren un comportamiento ético y profesional?	X				
	¿La empresa ha establecido un sistema de recompensa que promueva el cambio cultural deseable en el personal TI?	X				
1.5	**Supervisión del sistema de gobierno**				**EDM01.03**	NIA 315.A70 literal c)
	¿La empresa evalúa la efectividad y/o rendimiento del gerente de TI?	X				
	¿Existen evaluaciones si los mecanismos del gerente de TI operan efectiva en la estructura organizativa y los procesos y prácticas del gerente general?	X				
	¿Existen evaluaciones de las funciones del gerente TI para tomar acciones por cualquier desviación?	X				
	¿La empresa realiza una supervisión para determinar el punto hasta el que TI permite cumplir las obligaciones legales y contractuales?	X				
	¿La empresa realiza una supervisión para determinar el punto hasta el que TI permite cumplir las políticas de empresa?	X				
	¿La empresa realiza una supervisión para determinar el punto hasta el que TI permite cumplir las normas de contabilidad adoptadas?		X			
1.6	**El apetito por el riesgo o filosofía para la gestión del riesgo**					

1	ENTORNO DE CONTROL	SI	NO	N/A	COBIT 5	NIA
1.6.1	**Evaluación de la gestión de riesgos**				**EDM03.01**	NIA 315.A70 literal d)
	¿La entidad ha establecido el nivel de riesgo TI dispuesta a asumir para cumplir con sus objetivos?		X			
	¿Se han evaluado propuestas de tolerancia al riesgo frente a los niveles de oportunidad aceptables en las telecomunicaciones?		X			
	¿La entidad cuenta con mecanismos para alinear la estrategia de gestión de riesgos TI con la de riesgos de telefonía móvil?		X			
	¿La empresa evalúa los factores de riesgo de TI relacionadas con el comercio de paquetes de datos?		X			
	¿La empresa evalúa los factores de riesgo de TI relacionadas con el comercio de saldo electrónico?		X			
	¿Las decisiones empresariales se toman conscientes de los riesgos TI incorporados?		X			
	¿El uso de los recursos informáticos (servidores, kioscos, pos, sistemas operativos) está sujeto a valoración de riesgos según estándares?		X			
	¿El uso de los recursos informáticos (servidores, kioscos, pos, sistemas operativos) está sujeto a identificación de riesgos según estándares?		X			
1.7	**Orientación de la gestión de los riesgos**				**EDM03.02**	NIA 315.A70 literal d)
	¿La entidad promueve una cultura dirigida a concientizar al personal TI de los riesgos en los pines electrónicos y/o paquetes de datos?	X				
	¿La entidad promueve una cultura dirigida a impulsar la identificación proactiva de los riesgos TI en los pines electrónicos y/o paquetes de datos?	X				
	¿La entidad promueve una cultura dirigida a identificar oportunidades en el negocio de pines electrónicos y/o paquetes de datos?	X				

1	ENTORNO DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	¿Se encuentra integrada la estrategia de riesgos de TI con las operaciones de compra y venta de pines y/o paquetes de datos?		X			
	¿La empresa posee planes de comunicación de los riesgos TI identificados?		X			
	¿La empresa posee planes de acción de los riesgos TI identificados?		X			
	¿Los planes están implementados de tal manera que permiten responder rápidamente a los riesgos?			X		
	¿Los planes están implementados de tal manera que sean notificados inmediatamente a los niveles adecuados de gestión?			X		
	¿Los planes están implementados de tal manera que se encuentren soportados a través de principios escalados (que informar, cuando informar, dónde y cómo)?			X		
	¿La empresa es notificada por cualquier persona en cualquier momento acerca de los riesgos identificados en los pines electrónicos y/o paquetes de datos?		X			
	¿La empresa es notificada por cualquier persona en cualquier momento acerca de los problemas identificados en los pines electrónicos y/o paquetes de datos?	X				
	¿La empresa monitorea los indicadores clave para gestionar el riesgo?		X			
	¿Han sido aprobadas los adecuados enfoques, métodos y procesos para captura y notificación de riesgos?		X			
1.8	**Supervisión de la gestión de riesgos**				**EDM03.03**	NIA 315.A70 literal d)
	¿Es supervisado regularmente los umbrales de riesgo establecidos en el perfil global?		X			
	¿La empresa posee supervisión para verificar el alineamiento entre las metas y métricas del gerente TI con la gestión del riesgo?		X			

1	ENTORNO DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	En cuanto a la supervisión anterior ¿La empresa analiza las causas de las posibles desviaciones?		X			
	Al encontrar desviaciones ¿La empresa inicia medidas correctivas para abordar las causas?		X			
	¿La empresa facilita la revisión, por los dueños, del cumplimiento de objetivos del riesgo?		X			
	¿Se informa a la junta directiva de la empresa cualquier problema de gestión de riesgos en los pines electrónicos y/o paquetes de datos?		X			
1.9	**Estructura organizativa**					
1.9.1	**Definir la estructura organizativa**				**APO01.01**	NIA 315.A70 literal e)
	¿La empresa ha definido el alcance de la estructura organizativa de TI?	X				
	¿La empresa ha definido las funciones internas y externas de la estructura organizativa de TI?	X				
	¿La empresa ha definido las capacidades de decisión de la estructura organizativa de TI?	X				
	¿En la estructura organizativa de TI está claramente definidos quienes deben rendir cuentas?	X				
	¿En la estructura organizativa de TI está claramente definidos quienes son los responsables de los recursos?	X				
	¿Está alineada la estructura organizativa TI con la arquitectura corporativa?	X				
	¿Dentro de la estructura organizativa de TI existen responsabilidades para cada función?	X				
	¿La empresa posee un comité estratégico de TI a nivel de gerencias?		X			
	¿El comité se asegura de que la gerencia TI es el adecuado?			X		
	¿El comité se asegura de aconsejar sobre la dirección estratégica de TI?			X		

1	ENTORNO DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	¿El comité se asegura de revisar las inversiones en recursos TI tales como, equipos de cómputo, KIOSCOS y POS?			X		
	¿El comité se asegura de determinar las prioridades de comprar, de verificar el estado de los proyectos y resolver los conflictos entre recursos TI?			X		
	¿El comité se asegura de supervisar los servicios obtenidos por las TI?			X		
	¿La empresa ha definido reglas básicas de comunicación en la estructura TI?	X				
	¿Tales reglas básicas toman en cuenta la comunicación de arriba hacia abajo, abajo hacia arriba y de forma horizontal?	X				
	¿La comunicación entre la empresa y las funciones TI mantienen una estructura optima de enlace, comunicación y coordinación?	X				
	¿El gerente general verifica regularmente la adecuación de la estructura organizativa y la eficacia de TI?	X				
1.9.2	**Optimizar la ubicación de la función de ti**				**APO01.05**	NIA 315.A70 literal e)
	¿Las funciones del departamento de informática incluyen una evaluación de la importancia de los recursos TI?	X				
	¿Las funciones del departamento de informática han sido evaluadas para ser ubicadas en la organización?	X				
	¿Las funciones del departamento de informática han sido evaluadas para ser ubicadas en los modelos de aprovisionamiento (Adquisición)?	X				
	¿La ubicación de las funciones de TI ha sido aprobada?	X				
1.10	**Recursos humanos**					
1.10.1	**Mantener suficiente y adecuado la dotación de personal**				**APO07.01**	NIA 315.A70 literal g)
	¿Se realizan evaluaciones de las necesidades del personal en forma regular?	X				

1	ENTORNO DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	¿El departamento de informática cuenta con los recursos suficientes para apoyar las metas, objetivos empresariales y procesos de negocio?	X				
	¿Los procedimientos globales de la empresa están alineados con los procesos de contratación del personal TI?	X				
	¿Los procedimientos globales de la empresa están alineados con los procesos de retención del personal TI?	X				
	¿En el departamento de informática se asegura que existe un entrenamiento cruzado?		X			
	¿En el departamento de informática se asegura que existe respaldo para el personal clave para reducir dependencia?		X			
1.10.2	**Identificar personal clave de ti.**				**APO07.02**	NIA 315.A70 literal g)
	¿Para minimizar la dependencia de una sola persona en el departamento de informática la empresa captura/documenta el conocimiento de cada puesto?	X				
	¿Para minimizar la dependencia de una sola persona en el departamento de informática la empresa planifica la sucesión?		X			
	¿La empresa posee directrices sobre un tiempo mínimo de vacación anual que deben tomar los individuos clave?		X			
1.10.3	**Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio**				**APO07.05**	NIA 315.A70 literal g)
	¿La empresa maneja un inventario de recursos humanos del negocio?	X				
	¿La empresa maneja un inventario de recursos humanos del departamento informático?	X				
	¿La entidad identifica carencias de personal para elaborar procesos de contratación de personal informático?	X				

1	ENTORNO DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	¿La entidad cuenta con información adecuada para el tiempo dedicado a cada área y trabajo a realizar en informática?	X				
	¿La entidad cuenta con información adecuada para el tiempo dedicado a cada servicio TI?			X		
1.10.4	**Gestionar el personal contratado**				**APO07.06**	NIA 315.A70 literal g)
	¿Existen políticas relacionadas con el uso de consultores TI?		X			
	¿En tales políticas se ha establecido cuándo y cómo debe ser contratado?			X		
	¿En tales políticas se ha establecido que tipo de trabajo debe ser realizado?			X		
	¿El personal contratado ha firmado un acuerdo formal que indique su obligación de cumplir con el marco de control de TI?	X				
	¿El personal contratado ha firmado un acuerdo formal que indique su obligación de cumplir con el requisito de confidencialidad?					
	¿El personal contratado ha firmado un acuerdo formal que indique su obligación de cumplir con las políticas de seguridad física y lógica?	X				
	¿El personal de informática contratado es sujeto de inspecciones del gerente informático en cuanto al uso de correo electrónico y uso de programas y archivos de datos?	X				
	¿Se le ha proporcionado al personal de informática una definición clara de sus funciones, responsabilidad y requisitos para documentar su trabajo?	X				
	¿El trabajo del personal TI contratado es revisado?	X				
	¿Los pagos al personal de informática son basados en resultados?		X			
	¿El trabajo realizado por el personal informático está debidamente establecido en contratos?	X				

1	ENTORNO DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	¿La entidad realiza revisiones periódicas para asegurarse que el personal de informática tiene las funciones adecuadas?	X				
	¿La entidad realiza revisiones periódicas para asegurarse que el personal de informática tiene los derechos de acceso adecuados?	X				
1.10.5	**Información confidencial**					
	¿La entidad mantiene información confidencial en las transacciones con sus proveedores y clientes?	X				
	¿La entidad ha establecido acuerdos con sus proveedores y clientes para el manejo de tal información confidencial?	X				
	¿Qué tipo de información confidencial mantiene la entidad? - Contactos de clientes - Contactos de proveedores - Precios de compra - Precios de venta	 X X X X				

EVIDENCIA DE REVISIÓN:

	NOMBRE	FECHA	FIRMA
ELABORÓ	**Manuel Antonio Guardado Quintanilla**	**08/11/13**	
REVISÓ	**Oscar Alcides Montiel Hernández**	**08/11/13**	
AUTORIZÓ	**Ludwig Javier Guzmán Sosa**	**08/11/13**	

Fuente: elaboración propia.

2) Componente: el proceso de valoración del riesgo por la entidad.

Objetivo: conocer si la entidad tiene un proceso para la identificación de los riesgos de TI, la estimación de la relevancia de los riesgos, la valoración de su probabilidad de ocurrencia y la toma de decisiones con respecto a las actuaciones para responder a dichos riesgos.

La siguiente tabla muestra un resumen de los objetivos por cada elemento considerado en el cuestionario de 86 preguntas para verificación del proceso de valoración de riesgo por la entidad.

Tabla 7. Objetivos del componente: proceso de valoración del riesgo por la entidad.

No.	ELEMENTO	COBIT 5	NIA	OBJETIVO
2.1	**Gestionar el riesgo**			
2.1.1	**Recopilar datos**	APO12.01	NIA 315.15 literal a)	Obtener un conocimiento para saber si la entidad tiene un proceso para la identificación de los riesgos de negocio relevantes para los objetivos de la información financiera, como riesgos de TI.
2.1.2	**Analizar el riesgo**	APO12.02	NIA 315.15 literal b) y c)	Conocer si la entidad analiza la significatividad de los riesgos y valora la probabilidad de ocurrencia.
2.1.3	**Mantener un perfil de riesgo**	APO12.03	NIA 315.15 literal c)	Conocer si la entidad estima la significatividad de los riesgos y si mantiene un perfil de apetito por el riesgo.
2.1.4	**Expresar el riesgo**	APO12.04	NIA 315.15 literal d)	Indagar sobre la forma en que la entidad comunica las amenazas y oportunidades del riesgo a las partes interesadas y al nivel adecuado.
2.1.5	**Definir un portafolio de acciones para la gestión de riesgos**	APO12.05	NIA 315.15 literal d)	Verificar el abanico de soluciones o que la entidad ha establecido para responder a los riesgos y si estas son adecuadas.
2.1.6	**Responder al riesgo**	APO12.06	NIA 315.15 literal d)	Investigar sobre la toma de decisiones con respecto a las actuaciones para responder a dichos riesgos.

Fuente: elaboración propia.

Tabla 8. Cuestionario del componente: proceso de valoración del riesgo por la entidad.

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE:	PERIODO	REF.
RECARGA DIRECTA, S.A. DE C.V.	2012	

OBJETIVO:

Obtener entendimiento suficiente y adecuado sobre los riesgos de TI en la empresa, mediante la evaluación del control interno de la entidad, conforme a los componentes: ambiente de control; proceso de valoración del riesgo por parte de la entidad; sistemas de información comunicación; actividades de control y seguimiento de los controles. Ref. NIA 315.14 y COBIT.

PROCEDIMIENTOS:

Ejecute el siguiente cuestionario de conocimiento de los controles de TI mediante indagaciones ante la administración, de ser necesario realice comprobaciones de observación e inspección incluyendo procedimientos analíticos, como sustento a las respuestas de la entidad.

2	EL PROCESO DE VALORACIÓN DEL RIESGO POR LA ENTIDAD	SI	NO	N/A	COBIT 5	NIA
	Objetivo: conocer si la entidad tiene un proceso para la identificación de los riesgos de TI, la estimación de la significatividad de los riesgos, la valoración de su probabilidad de ocurrencia y la toma de decisiones con respecto a las actuaciones para responder a dichos riesgos.					
2.1	**Gestionar el riesgo**					
2.1.1	**Recopilar datos**				**APO12.01**	NIA 315.15 literal a)
	¿La empresa tiene un método para recoger, clasificar y analizar la información relacionada a riesgos informáticos?		X			
	¿Ese método utilizado por la entidad cubre múltiples tipos de eventos en los siguientes?			X		

2	EL PROCESO DE VALORACIÓN DEL RIESGO POR LA ENTIDAD	SI	NO	N/A	COBIT 5	NIA
	- Terminales POS - KIOSKOS - Servidores - Múltiples categorías y factores de riesgo.					
	¿En la gestión del riesgo informático se consideran los datos relevantes de los pedidos y entregas de PINES y paquetes de datos realizados a través de los KIOSCOS y POS?			X		
	¿La entidad mide y analiza los datos históricos de riesgo informático?			X		
	¿La entidad analiza los datos históricos de riesgo de informático?			X		
	¿Para analizar los datos históricos se considera las pérdidas experimentadas?			X		
	¿Para analizar los datos históricos se considera las tendencias de los clientes?	X				
	¿Para analizar los datos históricos se considera las tendencias de los proveedores?			X		
	¿Para analizar los datos históricos se considera las experiencias de la competencia?			X		
	¿Para analizar los datos históricos se considera las experiencias de las bases de datos de compra de pines y paquetes de datos?			X		
	¿Se han registrado datos sobre eventos de riesgo que han causado impactos en el software utilizado por los KIOSCOS?	X				
	¿Se han registrado datos sobre eventos de riesgo que han causado impactos en el software utilizado por los POS?	X				
	¿Se han registrado datos sobre eventos de riesgo que han causado impactos en el software utilizado por el servidor de la empresa?	X				

2	EL PROCESO DE VALORACIÓN DEL RIESGO POR LA ENTIDAD	SI	NO	N/A	COBIT 5	NIA
	¿Son capturados datos relevantes sobre incidentes en las compras y ventas de Pines y Paquetes de datos?	X				
	¿Son capturados datos relevantes sobre incidentes en los inventarios mantenidos por la entidad de pines y paquetes de datos?	X				
	¿Son capturados datos relevantes sobre problemas en las compras y ventas de Pines y Paquetes de datos?	X				
	¿Son determinadas las condiciones que existían cuando ocurrieron los eventos de riesgo?		X			
	¿Es analizado como afectan estas condiciones en la frecuencia del evento y la magnitud de la pérdida?		X			
	¿Se realiza periódicamente un análisis de los factores de riesgos? - En las terminales POS - KIOSKOS - Servidores		X			
	¿En cada análisis se logra identificar los un entendimiento de los factores de riesgo relacionados con el riesgo? - En las oficinas administrativas. - En las instalaciones donde están ubicados los Kioskos. - En las instalaciones donde están ubicados los POS.			X		
2.1.2	**Analizar el riesgo**				**APO12.02**	NIA 315.15 literal b) y c)
	¿Para el análisis de riesgos se ha definido puntualmente todas las transacciones? - POS - KIOSKOS - Servidores			X		

2	EL PROCESO DE VALORACIÓN DEL RIESGO POR LA ENTIDAD	SI	NO	N/A	COBIT 5	NIA
	¿En el análisis son considerados todos los factores de riesgo? - En los KIOSCOS. - En los POS. - En el Servidor - En las compras de pines y paquetes de datos. - En la venta de pines y paquetes de datos. - En la criticidad en el negocio de los recursos informáticos			X		
	¿La empresa construye regularmente escenarios de riesgo de TI? - se encuentran compuestos en cascadas. - consideran desarrollo de actividades de control. - consideran distintos tipos de amenaza coincidentes.		X			
	¿Para las pérdidas asociadas con escenarios de riesgo informático se estima la frecuencia de ocurrencia y la magnitud de la pérdida?			X		
	¿Al realizar estas estimaciones se toma en cuenta todos los factores de riesgo relevantes, la evaluación de controles conocidos y los niveles de riesgo residual?			X		
	¿Es comparado el riesgo residual con la tolerancia al riesgo?		X			
	¿Son identificadas las exposiciones que puedan requerir una respuesta al riesgo de los KIOSCOS y POS?			X		
	¿Se analiza el costo-beneficio de las opciones de respuesta al riesgo potencial?			X		
	¿En las opciones de respuesta al riesgo es considerado evitar, reducir y/o mitigar, transferir y/o compartir o aceptar el riesgo?			X		
	¿Al implementar respuestas a los riesgos, son especificados los requerimientos			X		

2	EL PROCESO DE VALORACIÓN DEL RIESGO POR LA ENTIDAD	SI	NO	N/A	COBIT 5	NIA
	necesarios de los proyectos y los controles a utilizar?					
	¿Antes de decidir sobre una respuesta al riesgo es considerado los resultados del análisis de riesgo?			X		
	¿Estos análisis son sujetos de comprobación con respecto a los requerimientos de la empresa?			X		
	¿Las estimaciones utilizadas en el análisis de riesgo son apropiadamente examinadas?			X		
2.1.3	**Mantener un perfil de riesgo**				**APO12.03**	NIA 315.15 literal c)
	¿La empresa lleva un inventario de las aplicaciones, infraestructura del sistema de información y proveedores de servicio de TI utilizadas por informática?	X				
	¿La empresa lleva un inventario de la?	X				
	¿Se ha determinado que servicios TI y recursos de infraestructura son esenciales para sostener la operación del negocio?	X				
	¿La empresa maneja escenarios de riesgo?		X			
	¿Los escenarios de riesgo son clasificados por categorías?			X		
	¿Se captura información sobre el perfil de riesgo en forma regular?		X			
	¿Esta información de perfil es consolidada en un perfil de riesgo acumulado?			X		
	¿La empresa ha identificado un conjunto de indicadores de riesgo?			X		
	¿La empresa ha identificado un conjunto de tendencias del riesgo?			X		
	¿La entidad maneja un registro de eventos de riesgo TI que se hayan materializado?	X				
	¿Estos registros de eventos son incluidos en el perfil de riesgo de TI empresarial?		X			
2.1.4	**Expresar el riesgo**				**APO12.04**	NIA 315.15 literal d)
	¿Son informadas a las partes interesadas todos los resultados del análisis de riesgo?		X			

2	EL PROCESO DE VALORACIÓN DEL RIESGO POR LA ENTIDAD	SI	NO	N/A	COBIT 5	NIA
	¿Para soportar decisiones de la empresa son realizados informes en términos entendibles y útiles?		X			
	¿Estos informes incluyen probabilidades de ocurrencia, rangos de pérdida y niveles de confianza?			X		
	¿Es proporcionada al gerente de informática los peores escenarios más probables?		X			
	¿Es informada a todas las partes interesadas? - El perfil de riesgo actual. - La efectividad del proceso de gestión de riesgos. - Efectividad de los controles. - Los cambios en el perfil de riesgo			X		
	¿Son revisados los resultados de evaluaciones realizadas por auditorías internas y por revisores de calidad?			X		
	¿En forma periódica son identificadas oportunidades relacionadas con TI que podrían permitir una aceptación de un mayor riesgo?			X		
2.1.5	**Definir un portafolio de acciones para la gestión de riesgos**				**APO12.05**	NIA 315.15 literal d)
	¿Para gestionar el riesgo la empresa mantiene un inventario de las actividades de control totales y en marcha?		X			
	¿Estas actividades permiten tomar riesgos alineados con el apetito y tolerancia de riesgo empresarial?			X		
	¿Las actividades de control se encuentran debidamente clasificadas y mapeadas de acuerdo al riesgo TI?			X		
	¿La entidad realiza una supervisión del riesgo?		X			
	¿Esta supervisión garantiza operar dentro de los niveles de tolerancia individual y general?			X		

2	EL PROCESO DE VALORACIÓN DEL RIESGO POR LA ENTIDAD	SI	NO	N/A	COBIT 5	NIA
	¿La empresa ha definido un conjunto de propuestas de proyecto diseñadas permitir lograr oportunidades estratégicas?		X			
2.1.6	**Responder al riesgo**				**APO12.06**	NIA 315.15 literal d)
	¿La empresa posee planes documentados de respuestas a cada riesgo?		X			
	¿Estos planes están sujetos a actualizaciones y pruebas?			X		
	¿Los planes documentados describen los pasos específicos y las vías de escalado ante un evento de riesgo?			X		
	¿Se comparan las exposiciones reales con los umbrales de tolerancia al riesgo?			X		
	Cuando ocurre un incidente de riesgo ¿Es aplicado el plan de respuesta apropiado?		X			
	¿Para determinar las causas de los incidentes son examinadas las pérdidas y oportunidades del pasado?		X			
	¿Son comunicados al gerente de informática las causas identificadas, propuestas adicionales y mejoras al proceso?		X			

EVIDENCIA DE REVISIÓN:

	NOMBRE	FECHA	FIRMA
ELABORÓ	**Manuel Antonio Guardado Quintanilla**	**11/11/13**	
REVISÓ	**Oscar Alcides Montiel Hernández**	**11/11/13**	
AUTORIZÓ	**Ludwig Javier Guzmán Sosa**	**11/11/13**	

Fuente: elaboración propia.

3) Componente: sistema de información y comunicación.

Objetivo: obtener un entendimiento del sistema de información, incluyendo los procesos de negocio relacionados, relevantes para la información financiera, de acuerdo a las siguientes áreas: Las clases de transacciones en las operaciones que son importantes para los estados financieros; los procedimientos de TI mediante los cuales las operaciones son iniciadas, registradas, procesadas y reportadas en los estados

financieros; los registros de contabilidad electrónicos, la información de respaldo. Así también la forma en que los sistemas de información capturan los eventos y las condiciones, diferentes a las clases de transacciones, que son significantes para los estados financieros; el proceso de información financiera usado para preparar los estados financieros de la entidad, incluyendo los estimados de contabilidad y las revelaciones significantes.

"El sistema de información financiera relevante para los objetivos de la información financiera, que incluye el sistema contable, comprende los procedimientos y registros diseñados y establecidos para:

- Iniciar, registrar y procesar las transacciones de la entidad (así como los hechos y condiciones) e informar sobre ellas, así como para rendir cuentas sobre los activos, pasivos y patrimonio neto correspondientes;
- Resolver el procesamiento incorrecto de transacciones, por ejemplo, ficheros de espera automatizados y procedimientos aplicados para reclasificar oportunamente las partidas pendientes de aplicación;
- Procesar y dar cuenta de elusiones del sistema o evitación de los controles;
- Transferir información desde los sistemas de procesamiento de las transacciones al libro mayor;
- Capturar información relevante para la información financiera sobre los hechos y las condiciones distintos de las transacciones, tales como la depreciación y la amortización de activos, así como los cambios en la recuperabilidad de las cuentas a cobrar; y
- Asegurar que se recoge, registra, procesa, resume e incluye adecuadamente en los estados financieros la información que el marco de información financiera aplicable requiere que se revele."

(IFAC, NIA 315, "Identificación y valoración de los riesgos de incorrección material mediante el conocimiento de la entidad y de su entorno, 2011, apartado A81)

La tabla siguiente muestra un resumen de los objetivos por cada elemento considerado en el cuestionario de 147 preguntas para verificación del sistema de información manejado por la entidad.

Tabla 9. Objetivos del componente del sistema de información y comunicación.

No.	ELEMENTO	COBIT 5	NIA	OBJETIVO
3.1	**Transacciones en las operaciones de la entidad.** (ver anexos 4, 5, 6 y 7)		NIA 315.18 lit. “a” y “b”. NIA 315.A81	Obtener conocimiento de los tipos de transacciones que son significativas para la información financiera, así como el procedimiento de iniciar, registrar y procesar las transacciones de la entidad.
3.2	**Corrección de errores**	DSS06.04	NIA 315.18 lit. “b” y “c”. NIA 315.A81	Indagar sobre los procedimientos para la corrección de errores y evitar la excesiva confianza en los sistemas.

No.	ELEMENTO	COBIT 5	NIA	OBJETIVO
3.3	**Valores parametrizables** Ver anexo 8.3	BAI10.01	NIA 315.A81	Verificar los hechos y condiciones distintas de las transacciones, tales como la depreciación y la amortización de activos, así como los cambios en la recuperabilidad de las cuentas a cobrar.
3.4	**Transferencia entre sistemas aislados**	BAI07.02 DSS06.02	NIA 315.A81	Asegurar que se recoge, registra, procesa y correctamente la información en el libro diario, cuando esta se migra de sistemas aislados o islas.
3.5	**Registro de eventos** Ver anexo 8.2	BAI03.05	NIA 315.A81	Investigar sobre las funciones del sistema para procesar y dar cuenta de elusiones del sistema o evitación de los controles, como pistas de auditoría, bitácora del sistema.
3.6	**Asientos en el libro diario**	APO01.08	NIA 315.A82	Revisar funciones en el sistema sobre partidas, recurrentes, automáticas, como inventarios, depreciaciones, amortizaciones, ventas, costo de ventas, inventarios, entre otros.
3.7	**Procesos de negocio relacionados cumplimiento de las disposiciones legales y reglamentarias.**	EDM01.01	NIA 315.A84	Revisar si la entidad ha definido actividades para evaluar los procesos de negocios relacionados con el cumplimiento de leyes y obligaciones y regulaciones.
3.7.1	**Sobre los puntos de venta.**	EDM01.01	NIA 315.A84	Revisar el cumplimiento de leyes mercantiles y tributarias sobre los puntos de venta KIOSKOS y POS.
3.7.2	**Del software de contabilidad**	EDM01.01	NIA 315.A84	Revisar los controles implementados para verificar lo adecuado, del sistema o software contable, a las leyes y regulaciones vigentes.

No.	ELEMENTO	COBIT 5	NIA	OBJETIVO
3.8	**Comunicación**	APO01.02	NIA 315.19; NIA 315.A86	Revisar como la entidad proporciona conocimiento de las funciones y responsabilidades individuales del control interno sobre la información financiera.
3.8.1	**Asignación de autoridad y delegación de responsabilidades. Establecer roles y responsabilidades.**	APO01.02	NIA 315.19; NIA 315.A86	Revisar como la entidad proporciona conocimiento de las funciones y responsabilidades individuales del control interno sobre la información financiera.

Fuente: elaboración propia.

Tabla 10. Cuestionario del componente sistemas de información y comunicación.

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE:	PERIODO	REF.
RECARGA DIRECTA, S.A. DE C.V.	2012	

OBJETIVO:

Obtener entendimiento suficiente y adecuado sobre los riesgos de TI en la empresa, mediante la evaluación del control interno de la entidad, conforme a los componentes: ambiente de control; proceso de valoración del riesgo por parte de la entidad; sistemas de información comunicación; actividades de control y seguimiento de los controles. Ref. NIA 315.14 y COBIT.

PROCEDIMIENTOS:

Ejecute el siguiente cuestionario de conocimiento de los controles de TI mediante indagaciones ante la administración, de ser necesario realice comprobaciones de observación e inspección incluyendo procedimientos analíticos, como sustento a las respuestas de la entidad.

3	SISTEMA DE INFORMACIÓN Y COMUNICACIÓN	SI	NO	N/A	COBIT 5	NIA
3.1	**Transacciones en las operaciones de la entidad.**					NIA 315.18 lit. “a” y “b”. NIA 315.A81
	Mediante indagaciones con el personal clave de la entidad conocer cómo se realiza el proceso de compras hasta su ingreso al inventario y pago al proveedor.	Ver anexo 4				
	¿Con que frecuencia realiza la entidad compras de recargas?	Semanalmente				
	¿Existe un procedimiento establecido para la compra de recargas?	X				
	¿Las compras de recargas son establecidas a través de una cantidad fija?		X			
	¿Las compras de recargas son establecidas a través de estimaciones?	X				
	¿La entidad utiliza intermediarios para realizar las compras de recargas?		X			
	¿El proveedor de recargas proporciona los inventarios al instante que son pedidos por la empresa?	X				
	¿Existen políticas de crédito establecidas por cada uno de los proveedores de la empresa?	X				
	¿Hay responsables por monitorear que los inventarios comprados al proveedor coincidan con las entradas al inventario?	X				
	¿El proveedor de recargas tiene acceso directo al servidor donde son almacenados los inventarios de recargas?	X				
	¿El suministro de los inventarios de recarga es realizado a través del internet?	X				
	¿Existen responsables de vigilar los inventarios mantenidos por la empresa en cada servidor?	X				
	¿Hay dispositivos de seguridad que protejan los saldos mantenidos en los servidores?	X				

3	SISTEMA DE INFORMACIÓN Y COMUNICACIÓN	SI	NO	N/A	COBIT 5	NIA
	¿Las personas que tienen acceso a la base de datos de inventarios están debidamente autorizadas?	X				
	¿Qué denominaciones compra la entidad para las recargas de saldos?	$1, $5, $10 Y $15				
	¿Qué denominaciones compra la entidad para las recargas de paquetes de datos?	256MB, 512MB, 1GB				
	Mediante indagaciones con el personal clave de la entidad conocer cómo se realiza el proceso de ventas hasta el pago del cliente.	Ver anexo 5				
	¿Existen mecanismos de seguridad aplicables al email entrante de pedidos?	X			Antivirus, Firewall.	
	¿La empresa efectúa frecuentemente levantamientos físicos de los POS?		X			
	¿Existen responsables del resguardo adecuado para cada POS?		X			
	¿El personal de clientes que utiliza los POS está debidamente adiestrado y autorizado para su uso?	X				
	¿La configuración de los POS es debidamente autorizado solo al administrador (técnicos de Recarga Directa?	X				
	¿Existen procedimientos para verificar los despachos realizados de saldo y paquetes a través de POS?		X			
	¿La entidad cuenta con planes de contingencia en casos de fallos en la red GPRS?		X			
	¿La tarjeta SIM de cada POS se encuentra debidamente resguardado, para evitar cualquier intento de sustracción no autorizada?		X			
	¿La entidad mantiene un monitoreo constante del flujo de datos intercambiados a través de cada POS?		X			
	¿Las tarjetas SIM utilizados por los POS son compatibles con teléfonos móviles?	X				

3	SISTEMA DE INFORMACIÓN Y COMUNICACIÓN	SI	NO	N/A	COBIT 5	NIA
	¿Existen medidas restrictivas para el intercambio de datos GPRS en teléfonos móviles?		X			
	¿La entidad ha realizado pruebas de descarga de datos en teléfonos móviles?		X			
	¿Cuenta la empresa con políticas de crédito de sus clientes?	X				
	¿El sistema ASPEL permite identificar aquellos clientes que infrinjan alguna política de crédito en particular?	X				
	¿La entidad cuenta con stock mínimo de inventario en saldo y paquetes de datos?	X				
	¿La empresa tiene procedimientos para la identificación y valuación de inventarios depositados en cada servidor?	X				
	¿Existe un responsable de conciliar la baja/salida de inventario versus lo facturado?		X			
	¿La entidad cuenta con la documentación que compruebe la propiedad de cada Kiosco?	X				
	¿Se realizan levantamientos físicos de cada Kiosco?		X			
	¿Existen responsables por el buen funcionamiento de cada Kiosco?	X				
	¿Existen responsables de conciliar las facturas emitidas por el Kiosco con cada despacho realizado?		X			
	¿Los Kioscos funcionan bajo la tecnología GPRS?	X				
	¿Cada Kiosco posee restricciones de acceso al sistema operativo o base de datos?	X				
	¿Existe un adecuado monitoreo del tráfico de datos de las tarjetas SIM con tecnología GPRS manejada por los Kioscos?		X			
	¿El consumidor (usuario) realiza la recarga por cuenta propia?	X				
	¿Existe un software especial para la interfaz del consumidor?	X				

3	SISTEMA DE INFORMACIÓN Y COMUNICACIÓN	SI	NO	N/A	COBIT 5	NIA
	¿El sistema es lo suficientemente capaz de interactuar con multiusuario al mismo tiempo?	X				
	¿Los consumidores (usuarios) realizan los pagos por recargas en efectivo?	X				
	¿Existen otros medios de pago distintos al efectivo?		X			
	¿El Kiosco lleva incorporado dispositivos de reconocimiento de distintas denominaciones de moneda?	X				
	¿Existe personal responsable del funcionamiento adecuado de las emisiones de tiquete?	X				
	¿Los inventarios de recargas que son despachados a través de Kioscos se encuentran almacenados en los servidores de la empresa?	X				
	¿Los usuarios poseen acceso implícito al inventario resguardado en los servidores?	X				
	Recargas no facturadas					
	¿La empresa tiene la seguridad que todos los despachos realizados de recargas son debidamente facturadas?		X			
	¿Existen controles relacionados para conciliar las recargas realizadas versus las facturaciones realizadas?		X			
	¿La empresa tiene antecedentes de recargas no facturadas?	X				
	¿Hubo un impacto considerable en los ingresos de la entidad resultantes de esas recargas no facturadas?	X				
	¿Existieron impactos en la disponibilidad del efectivo de la entidad por parte de esas recargas no facturadas?	X				
	¿Quién fue la persona o personas que detectaron tal irregularidad?	el jefe de informática				

3	SISTEMA DE INFORMACIÓN Y COMUNICACIÓN	SI	NO	N/A	COBIT 5	NIA
	¿Con que plazos tuvieron que ser canceladas las obligaciones contraídas con proveedores por esta causa?	60 días plazo				
	¿La disponibilidad de los inventarios resultó afectado por este incidente?	X				
	¿El número de quejas por clientes se incrementó por este problema?	X				
	¿Existieron clientes que se retiraron de la empresa por tal motivo?	X				
	¿Los tiquetes fueron impresos con posterioridad a la determinación del error?	X				
	¿La empresa declaró los ingresos a través de modificaciones de declaraciones?		X			
	Sustracción de tarjeta SIM					
	¿La entidad cuenta con medidas de seguridad de los POS?	X				
	¿Qué dispositivo utilizan para comunicarse los POS con el servidor?	Tarjeta SIM				
	¿Qué dispositivo utilizan para comunicarse los Kioscos con el servidor?	Tarjeta SIM				
	¿Qué tipo de tecnología de comunicación utiliza estas tarjetas SIM instalados en cada POS?	GPRS				
	¿Existen antecedentes perjudiciales para la entidad en cuanto al manejo de las tarjetas SIM?	X				
	¿La tarjeta SIM fue extraída por una persona autorizada?		X			
	¿Se dio aviso a la empresa de esta sustracción en forma oportuna?		X			
	¿Quién informó este hecho a la empresa recarga directa?	Empresa CLARO				
	¿Fueron utilizados los paquetes de descarga por parte del sustractor?	X				
	¿Fue limitada la descarga realizada por el sustractor?		X			
	¿Tiene conocimiento la entidad de cual POS fue la involucrada en este hecho?		X			

3	SISTEMA DE INFORMACIÓN Y COMUNICACIÓN	SI	NO	N/A	COBIT 5	NIA
	¿Cuánta cantidad de gigabytes fueron descargados sin autorización?	570GB				
	¿La empresa absorbió los costos de descarga en forma no autorizada?	X				
	¿La empresa cuenta con un procedimiento para este tipo de eventos?		X			
	¿Cuenta la entidad con pruebas tangibles de la veracidad de los hechos?		X			
	¿Los costos del evento afectaron los objetivos económicos de la entidad?	X				
	Recargas en temporadas promocionales					
	¿Los saldos y paquetes suministrados a los clientes están sujetos a promociones?	X				
	¿Qué tipo de promociones surgen?	Doble, Triple Saldo				
	¿La empresa cuenta con un procedimiento de venta ante promociones?	X				
	¿Existe un acuerdo comercial para cada promoción?	X				
	¿Los importes de bajas del inventario corresponden al acuerdo comercial de promoción?	X				
	¿La empresa proporciona saldo promocional?		X			
	¿El saldo promocional es proporcionado por la empresa de telecomunicaciones?	X				
	¿Existe algún tipo de irregularidades detectadas en el pasado con saldos y suministros promocionales?		X			
	¿La empresa cuenta con procedimientos para verificar cada venta de saldos y paquetes suministrados en temporadas de promoción?		X			
	¿Hay un responsable de notificar a la empresa telefónica o viceversa sobre cualquier promoción vigente?	X				
	Sensores Defectuosos					
	¿Los Kioscos funcionan con billetes?	X				

3	SISTEMA DE INFORMACIÓN Y COMUNICACIÓN	SI	NO	N/A	COBIT 5	NIA
	¿Los Kioscos funcionan con monedas?	X				
	¿Los kioscos poseen parametrizadas las distintas denominaciones de moneda y billetes?	X				
	¿Cuáles son los múltiplos de moneda que acepta el Kiosco?	$ 0.25, $1				
	¿Cuáles son los múltiplos de billetes que acepta el Kiosco?	$1, $5, $10				
	¿Los kioscos han reportado fallos en la detección de las distintas denominaciones de monedas y billetes?	X				
	¿Estas fallas son detectadas por la empresa al instante?		X			
	¿Existe personal responsabilizado en dar mantenimiento a los sensores de reconocimiento de monedas y/o billetes?	X				
	¿Con que frecuencia se realizan los mantenimientos preventivos y/o correctivos?	Anual				
	¿Es conciliado las recargas efectuadas por el kiosco versus el efectivo recolectado en ellos?	X				
	¿Son verificadas las ventas realizadas a través de tiquetes de los kioscos versus las salidas del inventario?	X				
	¿Los kioscos tienen provistos sistemas de alerta para indicar un stock máximo de efectivo, falta de conexión, falta de saldos y/o paquetes?	X				
	¿Son verificadas los ingresos reportados versus los tiquetes emitidos?	X				
	¿En caso de atasco de monedas y/o tiquetes, la empresa es informada al instante?		X			
	¿La cantidad de empleados en el departamento informático es suficiente para dar mantenimiento a los kioscos?	X				
	Describa el ciclo de la información contable en la empresa y que sistemas informáticos, personas e infraestructura de TI participan	Ver anexos 6 y 7				

3	SISTEMA DE INFORMACIÓN Y COMUNICACIÓN	SI	NO	N/A	COBIT 5	NIA
	en el periodo desde el origen hasta la presentación en los estados financieros					
3.2	**Corrección de errores**				**DSS06.04**	NIA 315.18 lit. "b" y "c". NIA 315.A81
	¿Existen procedimientos para identificar y corregir errores en el proceso automático de ventas de recargas POS y KIOSCOS? **Aseveraciones: O, E, Ex, I.**	X				
	¿Son almacenados los errores del sistema POSMOBILE y la familia de sistemas ASPEL que utiliza la entidad? **Aseveraciones: O.**	X				
	¿Son documentadas las medidas correctivas realizadas? **Aseveraciones: I.**	X				
3.3	**Valores parametrizables**	Ver anexo 8.3			**BAI10.01**	NIA 315.A81
	¿Existen responsables de parametrizar el sistema POSMOBILE y la familia del sistema ASPEL? **Aseveraciones: V, C.**	X				
	¿Existen perfiles de acceso a los campos de parametrización? **Aseveraciones: V, C.**	X				
	¿El monto mínimo de las recargas, establecido en el sistema de los KIOSCOS, es parametrizable? **Aseveraciones: V, C.**	X				
	¿El monto máximo de las recargas, establecido en el sistema KIOSCOS, es parametrizable? **Aseveraciones: V, C.**	X				
	¿Los encargados o autorizados de parametrizar el sistema ASPEL SAE 5.0 Y	X				

3	SISTEMA DE INFORMACIÓN Y COMUNICACIÓN	SI	NO	N/A	COBIT 5	NIA
	ASPEL COI y POSMOBILE cuentan con autoridad suficiente emanada según la posición en la estructura organizativa? **Aseveraciones: V, C.**					
	¿Qué información relevante para los estados financieros sobre hechos y condiciones distintas de las operaciones normales, con efecto en los estados financieros son parametrizables en los sistemas? **Aseveraciones: V, C.**					
	¿Los porcentajes de depreciación de los bienes de Propiedad, Planta y Equipo? **Aseveraciones: V, C, D.**	X				
	¿Corresponden a los valores del manual de políticas contables de la entidad? **Aseveraciones: V, C, D.**		X			
	¿Los porcentajes de amortización de los Activos Intangibles? **Aseveraciones: V, C, D.**	X				
	¿Corresponden a los valores del manual de políticas contables de la entidad? **Aseveraciones: V, C, D.**		X			
	¿Qué información relevante para los estados financieros son parametrizables entre los sistemas integrados de gestión y contabilidad? **Aseveraciones: V, C.**					
	¿Los porcentajes de impuestos en el módulo de ventas o captura de ingresos? **Aseveraciones: V, C, D.**	X				
	¿Los porcentajes de estimaciones de incobrabilidad de cuentas por cobrar? **Aseveraciones: V, C.**		X			
	¿Los porcentajes de retención y percepción de IVA de acuerdo al art. 162 y 163 del Código Tributario? **Aseveraciones: V, C, D.**		X			
	¿Se pueden establecer cuentas contables que sirva de enlace de cuentas entre el	X				

3	SISTEMA DE INFORMACIÓN Y COMUNICACIÓN	SI	NO	N/A	COBIT 5	NIA
	sistema administrativo y el sistema contable, como: inventarios, costo de ventas, devoluciones, entre otros? **Aseveraciones: V, C.**					
3.4	**Transferencia entre sistemas aislados**				**BAI07.02** **DSS06.02**	NIA 315.A81
	¿Se migra información financiera importante entre los sistemas de ventas al público POSMOBILE y el sistema de contabilidad ASPEL COI 6.0? **Aseveraciones: I, E, Ex.**	X				
	¿Qué tipo de información es transferida: ¿Costo de ventas? ¿Ventas o registro de ingresos? ¿Con que periodicidad se realizan? - A diario - Semanal - Mensual **Aseveraciones: I, E, Ex.**	 X X X				
	¿Se realizan verificaciones posteriores para verificar la integridad de la transferencia de información entre el sistema de ventas POSMOBILE y el sistema de contabilidad ASPEL COI 6.0? **Aseveraciones: I, E, Ex.**	X				
3.5	**Registro de eventos**	Ver anexo 8.2			**BAI03.05**	NIA 315.A81
	¿El sistema de puntos de venta POSMOBILE procesa y da cuenta de las elusiones del sistema o evitación de los controles mediante una bitácora o un registro electrónico de eventos? **Aseveraciones: I, Ex.**	X				
	¿El sistema de contabilidad ASPEL COI 6.0 procesa y da cuenta de las elusiones del sistema o evitación de los controles mediante una bitácora o un registro electrónico de eventos?	X				

3	SISTEMA DE INFORMACIÓN Y COMUNICACIÓN	SI	NO	N/A	COBIT 5	NIA
	Aseveraciones: I, Ex.					
	¿El sistema de administración ASPEL SAE 5.0 procesa y da cuenta de las elusiones del sistema o evitación de los controles mediante una bitácora o un registro electrónico de eventos? **Aseveraciones: I, Ex.**	X				
	¿La bitácora del sistema que registra las pistas de auditoría guarda información suficiente y adecuada, tales como? - Nombre del usuario. - Módulo afectado. - Hora y fecha del cambio. - Intentos de modificaciones de campos bloqueados. - Almacenamiento de las modificaciones de al menos los dos últimos años. **Aseveraciones: O.**	 X X X X	 X			
3.6	**Asientos en el libro diario**				**APO01.08**	NIA 315.A82
	¿Dentro del procesamiento de la información financiera que se realiza, permite el software de contabilidad partidas recurrentes, repetitivas y que se realicen de forma automática tales como? - Depreciación - Amortización. - Partidas de incobrabilidad sobre la base de saldos de clientes. - Costo de venta - Rebajas y devoluciones - Liquidación del IVA - Partidas de nóminas - Partidas de inventario (compras y ventas) - Otros (especifique) **Aseveraciones: O, E, Ex, I, D, V, C.**	 X X X X X X X X				

3	SISTEMA DE INFORMACIÓN Y COMUNICACIÓN	SI	NO	N/A	COBIT 5	NIA
	¿La empresa se ve implicada en utilizar asientos y estimaciones no estándar y no recurrentes en el proceso de registro de transacciones en el libro diario como los que se mencionan a continuación? - Ajustes de consolidación. - Combinación de negocios. - Deterioro de valor de los activos. **Aseveraciones: O, E, Ex, I, D, V, C.**	 X X X				NIA 315. A83
3.7	**Procesos de negocio relacionados cumplimiento de las disposiciones legales y reglamentarias.**				**EDM01.01**	NIA 315.A84
3.7.1	**Sobre los puntos de venta.**				**EDM01.01**	NIA 315.A84
	¿El sistema de puntos de venta esta adecuado con las leyes y regulaciones vigentes? **Aseveraciones: D.**	X				
	¿El sistema o aplicación POSMOBILE instalado en los kioscos o POS, tiene la capacidad técnica de emitir tiquetes en sustitución de facturas? **Aseveraciones: D.**	X				
	¿Se han agregado las nuevas sucursales en el F-210, para cada ubicación donde están instalados los puntos de venta? **Aseveraciones: D.**	X				
	¿Los sistemas de puntos de ventas han sido autorizados por la administración tributaria, cuentan con resolución individual y cartel de autorización? **Aseveraciones: D.**		X			
	¿Se ha colocado el cartel de autorización junto al kiosco en un lugar visible? (Art. 115 del Código Tributario) **Aseveraciones: D.**		X			
	¿Cuándo existe ajuste a operaciones documentadas con tiquete, se estampa por medio de un sello de hule en dicho tiquete la	X				

3	SISTEMA DE INFORMACIÓN Y COMUNICACIÓN	SI	NO	N/A	COBIT 5	NIA
	leyenda “Devolución” y al reverso del mismo consigna el nombre del cliente, firma, NIT o DUI? (Art. 46 del Reglamento de Aplicación del Código Tributario) **Aseveraciones: I, D.**					
	¿Las anulaciones o devoluciones se reflejan en negativo en la cinta de auditoría y se emite un nuevo tiquete de ser el caso? (Art. 46 del Reglamento de Aplicación del Código Tributario) **Aseveraciones: D, I.**	X				
	¿El Sistema de puntos de ventas POSMOBILE, permite emitir los reportes de ventas totales diarios(total z) y parciales (total x)? (Art 47 del Reglamento de Aplicación del Código Tributario) **Aseveraciones: D.**	X				
	¿El sistema de puntos de ventas POSMOBILE, registra las transacciones mediante un contador automático inviolable, que registre el número de tiquetes del día, sin perder el acumulado de ventas, y que pueda reiniciar cada día el contador de ventas sin perder el acumulado de tiquetes? (Art. 48 Reglamento del Código Tributario) **Aseveraciones: D, I, Ex.**	X				
	¿Las máquinas registradoras o sistemas computarizados están dotadas de una cinta de papel, rollo o cinta de auditoría que refleje al menos? - Las ventas y anulaciones. - Son copia fiel de los tiquetes originales. - Al inicio y al final de cada cinta de auditoría se imprime los datos del contribuyente. (Art. 48 Reglamento del Código Tributario) **Aseveraciones: D, I, Ex.**	X X X				
3.7.2	**Del software de contabilidad**				**EDM01.01**	NIA 315.A84

3	SISTEMA DE INFORMACIÓN Y COMUNICACIÓN	SI	NO	N/A	COBIT 5	NIA
	¿El software de contabilidad permite las siguientes figuras fiscales del país? - Retención 1% - Percepción 1% **Aseveraciones: D.**		X			
	¿El sistema ASPEL COI 6.0, permite los siguientes reportes? - Balance de Comprobación. - Libro Mayor. - Libro Diario- Mayor. - Balance General. - Estado de Resultados. (Art. 435 del Código de Comercio) **Aseveraciones: O, E, Ex, I, V, C, Co.**	 X X X X X				
	¿El sistema ASPEL SAE 5.0, permite adecuar el reporte de inventarios o kardex según los requerimientos de la Administración Tributaria? (Art. 142 del Código Tributario) **Aseveraciones: D, I.**		X			
	¿El sistema ASPEL SAE 5.0, automatiza los Libros de Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios? **Aseveraciones: D, I.**	X				
	¿Los reportes del ASPEL SAE 5.0 sobre los libros del Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios, emitidos por el sistema cumplen con los requisitos establecidos por el Código Tributario? **Aseveraciones: D, I.**	X				
3.8	**Comunicación**					
3.8.1	**Asignación de autoridad y delegación de responsabilidades. Establecer roles y responsabilidades.**				**APO01.02**	NIA 315.19; NIA 315.A86
	¿Cada función del departamento de informática ha establecido, acordado y	X				

3	SISTEMA DE INFORMACIÓN Y COMUNICACIÓN	SI	NO	N/A	COBIT 5	NIA
	comunicado roles individuales y las responsabilidades pertinentes?					
	¿Al momento de definir roles y/o responsabilidades se toma en cuenta los requisitos de la empresa y la competencia del personal?	X				
	¿La empresa mantiene registros actualizados de los roles y/o responsabilidades del departamento de informática?	X				
	¿La empresa mantiene registros actualizados de la información general del personal informático?	X				
	¿Los roles y/o responsabilidades están adheridos a las políticas de la gestión y procedimientos de TI?	X				
	¿La empresa ha implementado prácticas para asegurar que los roles y/o responsabilidades dispongan de suficientes recursos para ejecutarse y se pongan en práctica de forma correcta?	X				
	¿La gerencia de TI se aseguran que la rendición de cuentas están definidas en los roles de los técnicos de informática?	X				
	¿Los técnicos de informática se aseguran que la rendición de cuentas está definidas en sus responsabilidades?	X				

EVIDENCIA DE REVISIÓN:

	NOMBRE	FECHA	FIRMA
ELABORÓ	**Manuel Antonio Guardado Quintanilla**	**14/11/13**	
REVISÓ	**Oscar Alcides Montiel Hernández**	**14/11/13**	
AUTORIZÓ	**Ludwig Javier Guzmán Sosa**	**14/11/13**	

Fuente: elaboración propia.

4) Componente: actividades de control.

Objetivo: asegurar que se siguen las directrices de la dirección, tanto en los sistemas de TI como manuales, al respecto la NIA 315 establece:

"Para llegar a conocer las actividades de control de la entidad, el auditor obtendrá conocimiento del modo en que la entidad ha respondido a los riesgos derivados de las TI. La utilización de TI afecta al modo en que se implementan las actividades de control. Desde el punto de vista del auditor, los controles sobre los sistemas de las TI son eficaces cuando mantienen la integridad de la información y la seguridad de los datos que procesan dichos sistemas, e incluyen controles generales de las TI y controles de aplicaciones eficaces.

Los controles generales de las TI son políticas y procedimientos vinculados a muchas aplicaciones y favorecen un funcionamiento eficaz de los controles de las aplicaciones. Son aplicables en entornos con unidades centrales, redes de trabajo y de usuarios finales. Los controles generales de las TI que mantienen la integridad de la información y la seguridad de los datos generalmente incluyen controles sobre lo siguiente: a) centros de datos y operaciones de redes; b) adquisición, reposición y mantenimiento de software de sistemas; c) cambios en los programas.; d) seguridad de accesos; e) adquisición, desarrollo y mantenimiento de aplicaciones.

Los controles de aplicaciones son procedimientos manuales o automatizados que normalmente operan a nivel de procesos del negocio y que se aplican al procesamiento de las transacciones mediante aplicaciones específicas. Los controles de aplicaciones pueden ser preventivos o de detección y tienen como finalidad asegurar la integridad de los registros contables. En consecuencia, los controles de aplicaciones están relacionados con los procedimientos utilizados para iniciar y procesar transacciones y otros datos financieros, así como para informar sobre ellos. Estos controles ayudan a asegurar que las transacciones han ocurrido, están autorizadas y se han registrado y procesado íntegra y exactamente. Como ejemplos pueden citarse los filtros de datos de entrada y de secuencias numéricas con un seguimiento manual de los informes de excepciones o la corrección en el punto de entrada de datos."

(IFAC, NIA 315, "Identificación y valoración de los riesgos de incorrección material mediante el conocimiento de la entidad y de su entorno, 2011, apartado 21, A96 y A97)

La siguiente tabla muestra un resumen de los objetivos por cada elemento considerado en el cuestionario de 105 preguntas para verificación de las actividades de control.

Tabla 11. Objetivos del componente: actividades de control.

No.	ELEMENTO	COBIT 5	NIA	OBJETIVO
4.1 CONTROLES GENERALES				
4.1.1	**Seguridad de accesos**	APO13.01 DSS05.04	NIA 315.A56;A96	Verificar los controles generales establecidos para verificar la segregación de funciones y los perfiles de acceso de usuario en el sistema de información.
4.1.1.1	**Protección contra software maliciosos**	DSS05.01	NIA 315.A56;A96	Mantener la información libre de intrusos externos e internos, evitar cambios no autorizados en los datos de los archivos maestros.

No.	ELEMENTO	COBIT 5	NIA	OBJETIVO
4.1.2	**Cambios en los programas**	BAI06.01 DSS05.04	NIA 315.A56, A96.	Indagar la existencia de controles para evitar cambios no autorizados en los datos de los archivos maestros o cambios no autorizados en los sistemas o programas.
4.1.3	**Respaldos**	BAI06.01 DSS04.07	NIA 315.9; A56, anexo 1.9	Verificar la posible potencial pérdida de datos o incapacidad de acceder a los datos del modo requerido.
4.1.4	**Centro de datos y operaciones de redes**	BAI08.02 BAI09.03 BAI10.05 DSS01.04 DSS04.02 DSS05.05 MEA01.02	NIA 315.A56, A96.	Evaluar los controles de acceso físico a las instalaciones de TI, custodia de activos, entre otros.
4.2 CONTROLES DE APLICACIÓN				
4.2.1	**Origen de datos**	DSS05.05 DSS06.02	NIA 315.9, A97	Asegurar que las transacciones han ocurrido, sean auténticas y que los documentos o formularios fuentes estén pre numerados.
4.2.2	**Entrada de datos**	DSS05.05 DSS06.02	NIA 315.9, A97	Investigar si son contabilizadas las transacciones en el momento oportuno, que las partidas sean precisas, completas y válidas, incluyendo: filtros de entrada de datos, como máscaras, números negativos, fechas inconsistentes, entre otros.
4.2.3	**Proceso de datos**	DSS05.05 DSS06.02	NIA 315.9, A97	Indagar sobre la integridad y validez a través del procesamiento
4.2.4	**Salida de datos**	DSS05.05 DSS06.02	NIA 315.9, A97	Verificar en la entidad los controles para la precisión y completitud de la salida de información.

Fuente: elaboración propia.

Tabla 12. Cuestionario del componente: actividades de control.

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE:	PERIODO	REF.
RECARGA DIRECTA, S.A. DE C.V.	2012	

OBJETIVO:

Obtener entendimiento suficiente y adecuado sobre los riesgos de TI en la empresa, mediante la evaluación del control interno de la entidad, conforme a los componentes: ambiente de control; proceso de valoración del riesgo por parte de la entidad; sistemas de información comunicación; actividades de control y seguimiento de los controles. Ref. NIA 315.14 y COBIT.

PROCEDIMIENTOS:

Ejecute el siguiente cuestionario de conocimiento de los controles de TI mediante indagaciones ante la administración, de ser necesario realice comprobaciones de observación e inspección incluyendo procedimientos analíticos, como sustento a las respuestas de la entidad.

4	ACTIVIDADES DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	OBJETIVO: mantener la integridad de la Información y la Seguridad de los Datos mediante controles generales y controles de aplicación.					NIA 315.20 y 21. NIA 315.A95
4.1.1	**Seguridad de accesos**				**APO13.01** **DSS05.04**	NIA 315.A56;A96
	¿Existe un Sistema de Gestión de Seguridad de la Información SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio? **Aseveraciones: E, Ex, I.**	X				
	¿El sistema de gestión de seguridad de la información está alineado con los	X				

4	ACTIVIDADES DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	requerimientos de negocio y la gestión de seguridad en la empresa? **Aseveraciones: Todas**					
	¿El personal de TI está restringido a la posibilidad de obtener permisos de acceso más allá de los necesarios para realizar sus tareas? **Aseveraciones: E, Ex, I.**		X			
	¿El personal de TI carece de acceso para conocer las claves de acceso de los demás usuarios? **Aseveraciones: E, Ex, I.**	X				
	¿La administración de la sociedad carece de acceso a las contraseñas de los demás usuarios? **Aseveraciones: I.**	X				
	¿Está alineada política de gestión de identidades y derechos de acceso a los roles y responsabilidades definidos? **Aseveraciones: Todas.**	X				
	¿Tienen identificadas todas las actividades de proceso de la información por roles funcionales? **Aseveraciones: I.**	X				
	¿Mantienen autenticado todo acceso a los activos de información basándose en su clasificación de seguridad? **Aseveraciones: I.**	X				
	¿Cómo entidad administran todos los cambios de derechos de acceso (creación, modificación y eliminación)? **Aseveraciones: Todas.**	X				
	¿Poseen una segregación y gestión de cuentas de usuario privilegiadas? **Aseveraciones: Todas.**		X			
	¿Realizan regularmente revisiones de gestión de todas las cuentas y privilegios relacionados, por ejemplo: periodicidad de cambio de las contraseñas, longitud? **Aseveraciones: I.**	X				

4	ACTIVIDADES DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	¿Aseguran que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables de forma específica? **Aseveraciones: Ex.**	X				
	¿Mantienen una pista de auditoría de los accesos a la información clasificada como altamente sensible? **Aseveraciones: I.**	X				
	¿Las contraseñas de usuarios se almacenan en una base de datos segura? **Aseveraciones: I.**	X				
	¿Las claves de acceso de los usuarios del sistema cumplen con las siguientes características? - Caracteres en mayúsculas. - Caracteres en minúsculas. - Números. - Signos de puntación. - Caracteres especiales. **Aseveraciones: E.**	 X X X X X				
	¿Hay un mínimo de caracteres? **Aseveraciones: I.**	X				
	¿El sistema o software exige cambios periódicos de la contraseña? **Aseveraciones: I.**	X				
	¿Se almacena un historial de cambios de contraseña, que bloquee el intento de usar contraseñas previamente utilizadas? **Aseveraciones: I.**	X				
	¿Acceden múltiples personas a la base de datos? **Aseveraciones: I.**	X				
4.1.1.1	**Protección contra software maliciosos**				**DSS05.01**	NIA 315.A56;A96
	¿Cuentan con un plan y lo divulgan entre los empleados de TI para concientizar sobre el software malicioso?	X				

4	ACTIVIDADES DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	Aseveraciones: I, Ex.					
	¿Implementan procedimientos y definen responsabilidades de prevención ante software maliciosos? **Aseveraciones: I, Ex.**	X				
	¿Poseen instaladas y activadas herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente)? **Aseveraciones: I, Ex.**	X				
	¿Se encuentra distribuido todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios? **Aseveraciones: I.**	X				
	¿Efectúan revisiones y evaluaciones constantes sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad)? **Aseveraciones: I.**	X				
	¿Cuentan con filtros de seguridad ante entradas de correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing)? **Aseveraciones: I.**	X				
	¿Poseen plan de capacitación y formación periódica ante los usuarios de los sistemas sobre software malicioso en el uso del correo electrónico e internet? **Aseveraciones: Ex, I.**	X				
	¿Cuentan con un plan de formación hacia los usuarios de los sistemas para no instalarse software compartido o no autorizado? **Aseveraciones: Ex.**	X				
4.1.2	**Cambios en los programas**				**BAI06.01** **DSS05.04**	NIA 315.A56, A96.

4	ACTIVIDADES DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	¿La entidad cuenta con peticiones de cambio formales para posibilitar que los involucrados en el proceso de negocio y TI soliciten cambios en procesos de negocio, infraestructura, sistemas o aplicaciones y los cambios se realizan solo través de este proceso? **Aseveraciones: E.**	X				
	¿La entidad cuenta con un procedimiento documentado para declarar, evaluar, aprobar de formar preliminar, autorizar los cambios de emergencia en los programas y aplicaciones? **Aseveraciones: E, I.**	X				
	¿Los cambios de emergencia en los programas y sistemas son adecuadamente autorizados y documentados? **Aseveraciones: E.**	X				
	¿Existe un procedimiento para otorgar, cambiar/denegar permisos de acceso a los sistemas? **Aseveraciones: E.**	X				
	¿En el caso de cambios de sistema de información de la entidad, se ha realizado la correspondiente comprobación de, las cifras del nuevo sistema sean congruentes con las del cierre del antiguo sistema? **Aseveraciones: I, Ex.**			X		
4.1.3	**RESPALDOS.**				**BAI06.01** **DSS04.07**	NIA 315.9; A56, anexo 1.9
	¿La empresa cuenta con copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo a una planificación definida? **Aseveraciones: I, Ex.**	X				
	¿Qué tipo de información es respaldada? - Instaladores de los sistemas - Base de datos contables - Información administrativa (datos de clientes, proveedores)	 X X X				

4	ACTIVIDADES DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	- Bitácora del sistema **Aseveraciones: I, Ex.**	X				
	¿Con qué frecuencia se realizan? - Mensual - Semanal - Diaria - Etc. **Aseveraciones: I, Ex.**	X				
	¿Por cuál medio son guardadas las copias de seguridad? - Disco espejo - CD ROM - DVD - BLUE RAY - En la nube **Aseveraciones: I, Ex.**	X				
	¿Qué tipo de copias de seguridad maneja la empresa? - Completas - Incremental - Logarítmica **Aseveraciones: I, Ex.**	X				
	¿Los respaldos a los sistemas se encuentran encriptados? **Aseveraciones: I.**	X				
4.1.4	**Centro de datos y operaciones de redes**				**BAI08.02 BAI09.03 BAI10.05 DSS01.04 DSS04.02 DSS05.05 MEA01.02**	NIA 315.A56, A96.
	¿Existen procedimientos que permitan validar las fuentes de información? **Aseveraciones: I.**	X				
	¿La empresa ha establecido criterios de validación de la información de recargas? **Aseveraciones: I, Ex.**	X				
	¿Es verificado periódicamente las políticas necesarias que deben cumplir las bases de datos?	X				

4	ACTIVIDADES DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	Aseveraciones: I.					
	¿Estas políticas son comparadas con el estado actual físico y lógico de las bases de datos? **Aseveraciones: I.**	X				
	¿Para realizar esta comparación son utilizadas las herramientas apropiadas de inspección de los datos? **Aseveraciones: I.**	X				
	¿Es informado y revisado todas aquellas acciones aprobadas para eliminar información de las bases de datos? **Aseveraciones: I.**	X				
	¿Es verificado periódicamente si la información depositada en la base de datos corresponde a documentos que existen físicamente? **Aseveraciones: I.**	X				
	¿Es informado cualquier tipo de desviación entre la información de la base de datos y su existencia física? **Aseveraciones: I.**	X				
	¿La empresa ha establecido objetivos en función de la base de datos en cuanto a su completitud? **Aseveraciones: E.**	X				
	¿Es comparado periódicamente el nivel de completitud de la información respecto a los objetivos establecidos? **Aseveraciones: E.**	X				
	¿Son tomadas medidas para corregir cualquier desviación entre la completitud de la información en base de datos y la completitud según los objetivos establecidos? **Aseveraciones: E, I.**	X				
	¿Existen procedimientos de recuperación de la información garantizando la integridad de todos los datos? **Aseveraciones: I.**	X				
	¿Es evaluada la integridad de los datos recopilados por los sistemas POS MOBILE, ASPEL COI, ASPEL SAE? **Aseveraciones: I.**	X				

4	ACTIVIDADES DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	¿Los activos TI se encuentran inventariados por medio de un código individual, incluyendo el etiquetado físico? **Aseveraciones: Ex.**	X				
	¿Los activos se eliminan cuando no sirvan a ningún propósito útil debido a la finalización de todos los servicios relacionados, tecnología obsoleta o falta de usuarios? **Aseveraciones: Ex.**	X				
	¿Los activos de TI han sido asignados a los usuarios, con aceptación y firma de responsabilidades? **Aseveraciones: Ex.**	X				
	¿La empresa cuenta con perfiles de acceso actualizados? **Aseveraciones: Todas.**	X				
	¿El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) se basa en funciones previamente establecidas? **Aseveraciones: Todas.**	X				
	¿Se instruye a todo el personal para mantener visible la identificación en todo momento? **Aseveraciones: Todas.**	X				
	¿Se previene la expedición de tarjetas o placas de identidad sin la autorización adecuada? **Aseveraciones: Todas.**	X				
	¿Qué tipo de controles de acceso se utilizan para controlar al departamento informático? - Puertas de combinación de cifras - Claves de acceso - Lectores de tarjetas **Aseveraciones: Todas.**	X				
	¿Se restringe el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro tales como? - Vallas	X				

4	ACTIVIDADES DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	- Muros - Dispositivos de seguridad en puertas interiores y exteriores **Aseveraciones: I.**					
	¿Aseguran que los dispositivos registren el acceso y disparen una alama en caso de acceso no autorizado? - Placas o tarjetas llave - Teclados (keypads) - Circuitos cerrados de televisión - Escáneres biométricos **Aseveraciones: I.**	X				
	¿Disponen de registros de control de entrada y salida de personal visitante al área informática? **Aseveraciones: I.**	X				
	¿Se mantienen y supervisan de forma periódica a los dispositivos que detectan proactivamente las amenazas del entorno (p. ej. fuego, agua, humo, humedad)? **Aseveraciones: Todas.**	X				
	¿Los dispositivos están localizados en puntos claves del área de tecnología? **Aseveraciones: Todas.**	X				
	¿Disponen de protección de cables de red? **Aseveraciones: Todas.**	X				
	¿Existe un regulador de poder instalado y adecuadamente protegido contra fallos/interrupciones eléctricos? **Aseveraciones: Todas.**	X				
	¿Cada que tiempo se prueban las condiciones de la fuente de poder o UPS? - Mensualmente - Trimestralmente - Semestralmente - Anualmente **Aseveraciones: Todas.**	X				
	¿Están los equipos de humo y fuego certificados por técnicos reconocidos? **Aseveraciones: Todas.**	X				

4	ACTIVIDADES DE CONTROL	SI	NO	N/A	COBIT 5	NIA
4.2	**Controles de aplicación**				**DSS05.05 DSS06.02**	NIA 315.9, A97
4.2.1	**Origen de datos**				**DSS05.05 DSS06.02**	NIA 315.9, A97
	¿Las transacciones ingresadas por los individuos se hacen siguiendo los procedimientos establecidos, incluyendo, cuando sea apropiado, la adecuada segregación de tareas en relación al origen y aprobación de esas transacciones? **Aseveraciones: O, E, Ex, I.**	X				
	¿Se verifica la autenticidad de la información fuente de las transacciones y que él o ella tienen la autoridad para originar las transacciones? **Aseveraciones: O, E, Ex.**	X				
	¿Hacen uso de documentos pre impresos para alimentar el sistema? **Aseveraciones: I.**	X				
	¿Hacen uso de formularios completados a mano para alimentar el sistema? **Aseveraciones: I.**		X			
	¿Dichos documentos o formularios se encuentran elaborados de acuerdo a la secuencia de ingreso al sistema? **Aseveraciones: I.**	X				
	¿Están bien identificados y numerados? **Aseveraciones: E, I.**	X				
	¿Presentan títulos encabezados descriptivos? **Aseveraciones: O, E.**	X				
	¿Poseen espacio suficiente para correcciones y firmas de responsables? **Aseveraciones: I.**	X				
	¿Los datos se contabilizan en el instante en que ocurre el evento? **Aseveraciones: O.**		X			
	¿Son contabilizados por comunicación verbal? **Aseveraciones: O, V.**		X			

4	ACTIVIDADES DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	¿Son contabilizados por comunicación telefónica? **Aseveraciones: O, V.**		X			
	¿Son contabilizados a través de otra aplicación? **Aseveraciones: O, V.**	X				
4.2.2	**Entrada de datos**				**DSS05.05** **DSS06.02**	NIA 315.9, A97
	¿Se contabilizan transacciones del negocio en el momento oportuno? **Aseveraciones: O.**	X				
	¿Se verifica si las partidas de diario son precisas, completas y válidas con respecto a los documentos fuente? **Aseveraciones: E, Ex, I.**	X				
	¿Se validan los datos de entrada y la edición o, cuando sea aplicable y la devolución para su corrección tan cerca al punto de origen como sea posible? **Aseveraciones: I.**	X				
	¿El sistema evita introducir información diferente a la requerida en los formularios de ingreso de datos? **Aseveraciones: O, Ex.**	X				
	¿En los campos numéricos está bloqueado el ingreso de números negativos donde no correspondan? **Aseveraciones: O, Ex.**	X				
	¿Las máscaras de entrada de datos se encuentran bien definidas y no admiten el ingreso de datos incongruentes (Ej.: días, meses, años inválidos)? **Aseveraciones: O, Ex.**	X				
	En algún momento, ¿se requieren de modificaciones en los valores que se obtienen por cálculos automáticos? **Aseveraciones: O, Ex.**		X			
4.2.3	**Proceso de datos**				**DSS05.05** **DSS06.02**	NIA 315.9, A97

4	ACTIVIDADES DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	¿Se mantiene la integridad y validez de los datos a través del ciclo de procesamiento? - Recargas POS - Recargas Kioscos - Compras **Aseveraciones: I.**	 X X X				
	¿Cuentan con procedimientos para la verificación de la integridad y consistencia de toda la información almacenada en el sistema, exclusivamente en todos aquellos módulos relacionados con la información contable y financiera? **Aseveraciones: Ex, I.**		X			
	¿Se aseguran que la detección de transacciones erróneas no interrumpe el procesamiento de las transacciones válidas? **Aseveraciones: I, V.**	X				
	¿Se mantiene la integridad de los datos durante interrupciones no esperadas en el procesamiento de negocio? **Aseveraciones: I.**	X				
	¿Cuentan con un plan de acciones correctivas en el caso que se den fallas en el sistema sin que se interrumpa el proceso de las transacciones válidas? **Aseveraciones: Todas.**	X				
	¿Se confirma la integridad de los datos después de los fallos de procesamiento? **Aseveraciones: I.**	X				
	¿Se verifica de forma manual, la exactitud aritmética de los registros del sistema, es decir, que las sumatorias de la información que el sistema muestra corresponden a la información real? **Aseveraciones: Ex, E.**	X				
	¿Poseen alguna política de verificación de que los saldos de un nuevo periodo correspondan a los finales del periodo anterior?		X			

4	ACTIVIDADES DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	Aseveraciones: I, Ex.					
	¿En el caso que se hagan correcciones de transacciones erróneas, sólo son ejecutadas por una persona autorizada (el encargado)? **Aseveraciones: Todas.**	X				
4.2.4	**Salida de datos**				**DSS05.05** **DSS06.02**	NIA 315.9, A97
	¿La salida de la información se da de una forma autorizada, se entrega al beneficiario apropiado y se protege la información durante la transmisión? **Aseveraciones: I, Ex.**	X				
	¿Se verifica la precisión y completitud de la salida? **Aseveraciones: I, Ex.**	X				
	Cuando se transfieren datos de la transacción entre las aplicaciones internas y las funciones operacionales o de negocio (dentro o fuera de la organización), ¿Se comprueba el correcto direccionamiento, autenticidad de origen e integridad del contenido? **Aseveraciones: I, Ex, E.**	X				
	¿Se mantiene la autenticidad e integridad durante la transmisión o la generación del informe? **Aseveraciones: I, Ex.**	X				
	¿Los informes finales que genera el sistema son necesarios y suficientes para la toma de decisiones y el cumplimiento del objetivo organizacional? **Aseveraciones: I, V.**		X			
	¿Los reportes generados por el sistema se encuentran bien identificados, conforme a las necesidades de los usuarios de la información (título, fecha, periodo cubierto, entre otros)? **Aseveraciones: Ex.**	X				

4	ACTIVIDADES DE CONTROL	SI	NO	N/A	COBIT 5	NIA
	¿Los informes emitidos por el sistema son procesados y entregados a los niveles jerárquicos correspondientes? **Aseveraciones: I.**	X				
	¿Los reportes son íntegros con respecto a la información manejada por el sistema y las necesidades de la compañía? **Aseveraciones: I.**	X				
	¿Los usuarios pueden editar los informes generados y guardados por el sistema? Nota: esto es porque aplicaciones pueden generar reportes y guardarlos en un lugar específico de la terminal para posteriormente ser impresos. **Aseveraciones: I, Ex, V.**	X				
	¿Existe algún manual en donde se especifique algún procedimiento que aplique la entidad para la destrucción o almacenamiento adecuado de los reportes con información restrictiva o confidencial? **Aseveraciones: Ex.**	X				

EVIDENCIA DE REVISIÓN:

	NOMBRE	FECHA	FIRMA
ELABORÓ	**Manuel Antonio Guardado Quintanilla**	**17/11/13**	
REVISÓ	**Oscar Alcides Montiel Hernández**	**17/11/13**	
AUTORIZÓ	**Ludwig Javier Guzmán Sosa**	**17/11/13**	

Fuente: elaboración propia.

5) Componente: seguimiento de controles.

Objetivo: conocer las principales actividades que la entidad lleva a cabo para realizar un seguimiento del control interno TI relativo a la información financiera y relevante a la auditoria. Conlleva la valoración oportuna de la eficacia de los controles y la adopción de las medidas correctoras necesarias.

La siguiente tabla muestra un resumen de los objetivos por cada elemento considerado en el cuestionario de 50 preguntas para verificación de los seguimientos de los controles.

Tabla 13. Objetivos del componente seguimiento de controles.

No.	ELEMENTO	COBIT 5	NIA	OBJETIVO
5.1	**Supervisar y evaluar el sistema de control interno TI.**			Verificar el seguimiento oportuno y evaluación de los controles establecidos.
5.1.1	**Supervisar y hacer controles y revisiones de calidad.**	APO11.04	NIA 315.22 NIA 315.A98	Supervisar el establecimiento de la calidad en los procesos y servicios de forma permanente.
5.1.2	**Supervisar el control interno TI**	MEA02.01	NIA 315.22	Realizar, de forma continua, la supervisión, los estudios comparativos y la mejora el entorno de control de TI y el marco de control para alcanzar los objetivos organizativos.
5.1.3	**Revisar la efectividad de los controles sobre los procesos de negocio.**	MEA02.02	NIA 315.22	Revisar la operación de controles, incluyendo la revisión de las evidencias de supervisión y pruebas, para asegurar que los controles incorporados en los procesos sean efectivos.
5.1.4	**Realizar autoevaluaciones de control.**	MEA02.03	NIA 315.24	Revisar el modo en que la sociedad realiza procedimiento de mejora del control, a través de programas continuos de autoevaluación que valoren la completitud y efectividad del control de la dirección sobre los procesos de TI.
5.1.5	**Identificar y comunicar las deficiencias del control de TI.**	MEA02.04	NIA 315.22	Identificar el modo en que las deficiencias de control son analizadas e identificadas con las causas raíz subyacentes. Verificar la comunicación de las deficiencias a las partes interesadas.

Fuente: elaboración propia.

Al haber realizado estas actividades de indagación y sus correspondientes procedimientos analíticos, los auditores obtienen el entendimiento del control interno exigido por la NIA 315, con tal resultado se procederá a visualizar todas aquellas preguntas con respuesta negativa para la identificación de riesgos, los cuales se presentan en el siguiente paso.

Tabla 14. Cuestionarios del componente seguimiento de controles

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE:	PERIODO	REF.
RECARGA DIRECTA, S.A. DE C.V.	2102	

OBJETIVO:

Obtener entendimiento suficiente y adecuado sobre los riesgos de TI en la empresa, mediante la evaluación del control interno de la entidad, conforme a los componentes: ambiente de control; proceso de valoración del riesgo por parte de la entidad; sistemas de información comunicación; actividades de control y seguimiento de los controles. Ref. NIA 315.14 y COBIT.

PROCEDIMIENTOS:

Ejecute el siguiente cuestionario de conocimiento de los controles de TI mediante indagaciones ante la administración, de ser necesario realice comprobaciones de observación e inspección incluyendo procedimientos analíticos, como sustento a las respuestas de la entidad.

5	SEGUIMIENTO DE CONTROLES	SI	NO	N/A	COBIT 5	NIA
	Objetivo: conocer las principales actividades que la entidad lleva a cabo para realizar un seguimiento del control interno TI relativo a la información financiera y relevante a la auditoria.					
5.1	**Supervisar y evaluar el sistema de control interno TI**					
5.1.1	**Supervisar y hacer controles y revisiones de calidad**	**X**			**APO11.04**	**NIA 315.22 NIA 315.A98**
	¿Se realiza una supervisión de la calidad de los procesos de control informático en forma permanente y sistemática?	X				

5	SEGUIMIENTO DE CONTROLES	SI	NO	N/A	COBIT 5	NIA
	¿Cada supervisión es realizada mediante las métricas de control TI?	X				
	¿Son llevados a cabo revisiones de calidad del control informático?	X				
	¿Con la información obtenida de las supervisiones es realizado el respectivo informe?	X				
	¿Con la información obtenida de las supervisiones son puestas en marcha las mejoras correspondientes?	X				
	¿Son supervisadas las métricas de calidad de los procesos de control informático?	X				
	¿La supervisión es realizada basada en objetivos generales de calidad, en todos los servicios y proyectos individuales?	X				
	¿Las revisiones son realizadas por un delegado del gerente de informática?	X				
	¿Las revisiones son realizadas por el encargado del proceso TI?		X			
	¿Son analizados los resultados del rendimiento de la gestión de calidad?	X				
5.1.2	**Supervisar el control interno TI**				**MEA02.01**	NIA 315.22
	¿El control interno informático es sujeto de evaluaciones?	X				
	¿Estas actividades se basan en los estándares de Gerente TI y los marcos de referencia?	X				
	¿Las actividades de supervisión del control interno son sujetas de un seguimiento adecuado y de una evaluación de la eficiencia y efectividad de tal revisión?	X				
	¿La entidad considera las evaluaciones independientes del sistema de control interno?		X			

5	SEGUIMIENTO DE CONTROLES	SI	NO	N/A	COBIT 5	NIA
	¿Se ha identificado puntualmente los límites del sistema de control interno?		X			
	¿La empresa se asegura de que las actividades de control están en funcionamiento?	X				
	¿Cuándo existe una actividad de control que no está en funcionamiento la entidad lo comunica oportunamente, le da un seguimiento y análisis especial?	X				
	¿Cuándo existe una actividad de control que no está en funcionamiento la entidad implementa las acciones correctivas oportunas?	X				
	¿El sistema de control interno es actualizado ante la ocurrencia de cambios en el curso del negocio y cambios en el riesgo de TI?		X			
	¿El rendimiento del marco de control es evaluado regularmente?		X			
	¿La evaluación anterior incluye un estudio comparativo con los estándares?			X		
	¿La evaluación anterior incluye un estudio comparativo con las buenas prácticas aceptadas por la industria?			X		
	¿La entidad ha adoptado un enfoque para la mejora continua del control interno?	X				
5.1.3	**Revisar la efectividad de los controles sobre los procesos de negocio**				**MEA02.02**	NIA 315.22
	¿Los riesgos de TI son comprendidos por la organización?	X				
	¿Los riesgos de TI son priorizados por la organización?	X				

5	SEGUIMIENTO DE CONTROLES	SI	NO	N/A	COBIT 5	NIA
	¿Para efectos de validar controles se han identificado los controles clave?	X				
	¿Para efectos de validar controles se ha desarrollado una estrategia adecuada?	X				
	¿La entidad identifica información convincente si el control interno está operando en forma efectiva?	X				
	¿La entidad posee evidencia de la efectividad del control interno?	X				
5.1.4	**Realizar autoevaluaciones de control**				**MEA02.03**	NIA 315.24
	¿Se realizan autoevaluaciones de control?	X				
	¿Estas autoevaluaciones incluyen planes de autoevaluación?	X				
	¿Estas autoevaluaciones incluyen un alcance?	X				
	¿Estas autoevaluaciones incluyen criterios de evaluación?	X				
	¿Los resultados de las autoevaluaciones son comunicados al gerente general?	X				
	¿Son considerados los estándares de auditoria interna en el diseño de las autoevaluaciones?	X				
	¿Existen responsables de realizar las autoevaluaciones?	X				
	¿Son realizadas revisiones independientes?		X			
	¿Estas revisiones permiten asegurar la objetividad de la autoevaluación?			X		
	¿Estas revisiones permiten compartir las buenas prácticas de control interno con otras compañías?			X		

5	SEGUIMIENTO DE CONTROLES	SI	NO	N/A	COBIT 5	NIA
	¿Los resultados de las autoevaluaciones son comparadas con los estándares?	X				
	¿Los resultados de las evaluaciones permiten considerar acciones correctivas?	X				
5.1.5	**Identificar y comunicar las deficiencias del control de TI**				**MEA02.04**	NIA 315.22
	¿Las deficiencias de control interno son identificadas, comunicadas y registradas estadísticamente?	X				
	¿Existen responsables para resolver las deficiencias y comunicar los resultados de resolución?	X				
	¿La entidad comunica adecuadamente los procedimientos de análisis de causas?	X				
	¿La entidad comunica adecuadamente los procedimientos de comunicación a los técnicos en informática apropiados?	X				
	¿Se ha definido que deficiencias comunicar a la persona responsable de la función?	X				
	¿Se ha definido que deficiencias comunicar a los gerentes correspondientes?	X				
	¿Se ha definido que deficiencias comunicar a los técnicos en informática?	X				
	¿La empresa da un seguimiento de todas las deficiencias para asegurar que se han seguido los adecuados planes de acción?	X				
	¿Las acciones correctivas que surgen de la evaluación de control son identificadas claramente, rastreadas e implementadas?	X				

EVIDENCIA DE REVISIÓN:

	NOMBRE	FECHA	FIRMA
ELABORÓ	**Manuel Antonio Guardado Quintanilla**	**20/11/13**	
REVISÓ	**Oscar Alcides Montiel Hernández**	**20/11/13**	
AUTORIZÓ	**Ludwig Javier Guzmán Sosa**	**20/11/13**	

Fuente: elaboración propia.

Los componentes de “sistema de información” y “actividades de control” están directamente relacionadas con las aseveraciones que realiza la administración sobre la información financiera que es auditada; para efectos de identificar puntualmente cada una de ellas se ha procedido a referenciar, en cada interrogante las afirmaciones con las cuales se relacionan. Tales preguntas hacen énfasis a las abreviaciones de la tabla 16.

3.3.3 Paso 3: identificación y evaluación de riesgos

Para identificar riesgos es preciso localizar todas aquellas debilidades del control interno que según COBIT 5 existen en la entidad, estas debilidades están expresadas mediante todas aquellas preguntas en cuya respuesta se obtuvo un resultado negativo.

A continuación se presenta listado de todas las debilidades encontradas, referenciadas a cada elemento del componente control interno especifico, paralelamente se hace una breve descripción del riesgo identificado para cada vulnerabilidad.

Tabla 15. Listado de debilidades encontradas en el control interno de TI.

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE:	PERIODO	REF.
RECARGA DIRECTA, S.A. DE C.V.	2012	

OBJETIVO:

Presentar las debilidades encontradas en el diseño del control interno de TI en la empresa.

REF.	ÁREA	DEBILIDADES DEL CONTROL INTERNO	RIESGOS IDENTIFICADOS
ENTORNO DE CONTROL DE TI			
1.2	Compromiso por la competencia	Inexistencia de una formación profesional del personal en tecnología.	Paralización de las operaciones del negocio por retiro, enfermedad y/o fallecimiento del personal.
1.2	Compromiso por la competencia	Ausencia de planes para sucesión del personal clave	Paralización de las operaciones del negocio por retiro, enfermedad y/o fallecimiento del personal.
1.2	Compromiso por la competencia	La empresa no ha desarrollado programas de formación de conocimiento (incluido el control interno) dirigidas al personal.	Incapacidad de los encargados de tecnología de adaptarse a los cambios del entorno.
1.5	Supervisión del sistema de gobierno	Falta de supervisión para asegurar que la tecnología de información ayuda en el cumplimiento de los marcos de contabilidad adoptados.	Incumplimiento de políticas contables
1.6	Evaluación de la gestión de riesgos	Ausencia de un nivel de riesgo que la entidad esté dispuesta asumir para cumplir con sus objetivos	Alta vulnerabilidad en todos los recursos informáticos.
1.6	Evaluación de la gestión de riesgos	Inexistencia de evaluaciones de factores de	Alta vulnerabilidad en todos los recursos de TI.

REF.	ÁREA	DEBILIDADES DEL CONTROL INTERNO	RIESGOS IDENTIFICADOS
		riesgo en las operaciones del negocio	
1.7	Orientación de los riesgos	Falta de comunicación con respecto a los riesgos identificados	Incapacidad de alcanzar los objetivos.
1.7	Orientación de los riesgos	Falta de planes de acción con respecto a los riesgos	Información financiera no razonable.
1.9.1	Orientación de los riesgos	Ausencia de un comité estratégico	Incapacidad de gestionar los riesgos relevantes a la información financiera.
1.10.1	Mantener suficiente y adecuado la dotación del personal TI	Falta de entrenamiento cruzado entre el personal	Dependencia de procesos críticos en una sola persona.
1.10.3	Planificar y realizar un seguimiento del uso de recursos humanos de TI	Desconocimiento del tiempo dedicado a cada función del personal.	Respuestas al riesgo en forma inoportuna.
EL PROCESO DE VALORACIÓN DE RIESGO DE TI POR LA ENTIDAD			
2.1.1	Recopilar datos	Falta de un método para recoger, clasificar y analizar la información relacionada a los riesgos.	Falta de comprensión de los riesgos de tecnología y su impacto en la información financiera.
2.1.1	Recopilar datos	No existe análisis sobre las condiciones existentes ante el surgimiento de un evento de riesgo	Incapacidad de predecir riesgos futuros.
2.1.2	Analizar el riesgo	Ausencia de escenarios de riesgo	Falta de preparación o de planes para reaccionar a los riesgos de tecnología.
2.1.2	Analizar el riesgo	No hay comparación entre el riesgo residual y la tolerancia al riesgo.	Incomprensión de los riesgos aceptados versus los riesgos residuales permitidos por los controles implementados.
2.1.3	Mantener un perfil de riesgo	Ausencia de un perfil de riesgo en la entidad	Falta de preparación o de planes para reaccionar a los riesgos de tecnología.
2.1.4	Expresar el riesgo	Falta de comunicación a las partes interesadas sobre la gestión de riesgo	Respuestas inapropiadas o nulas de las partes interesadas(gerente de TI, accionistas o junta directiva) ante los riesgos detectados
2.1.4	Expresar el riesgo	No se elaboran peores escenarios más probables	Falta de preparación o de planes para reaccionar a los riesgos de tecnología

REF.	ÁREA	DEBILIDADES DEL CONTROL INTERNO	RIESGOS IDENTIFICADOS
			sobre los peores escenarios más probables.
2.1.4	Expresar el riesgo	Ausencia de informes hacia las partes interesadas relativas a la efectividad de los controles	Respuestas inapropiadas o nulas de las partes interesadas (gerente de TI, accionistas o junta directiva) para la mejora de los controles.
2.1.5	Definir un portafolio de acciones para la gestión de riesgos	Falta de un inventario de actividades de control para la gestión de riesgos TI	Respuestas inapropiadas o nulas de las partes interesadas(gerente de TI, accionistas o junta directiva) ante los riesgos detectados
2.1.5	Definir un portafolio de acciones para la gestión de riesgos	Ausencia de supervisión de riesgos.	Falta de observación del origen de los riesgos, el impacto en la empresa y la forma en que se mitiga.
2.1.6	Responder al riesgo	Falta de respuestas a realizar para cada riesgo en particular	Respuestas inapropiadas o nulas de las partes interesadas(gerente de TI, accionistas, gerente o junta directiva) ante los riesgos detectados
SISTEMA DE INFORMACIÓN Y COMUNICACIÓN			
3.3	Valores parametrizables	Los porcentajes de depreciación y amortización no corresponden a las políticas contables de la entidad	Procesamiento inexacto de las depreciaciones y amortizaciones por parte del sistema.
3.3	Valores parametrizables	No es posible parametrizar los porcentajes de estimación para cuentas incobrables.	Inadecuada valuación de las estimaciones, cuentas por cobrar inexistentes.
3.3	Valores parametrizables	No es posible parametrizar los porcentajes de retención y percepción del impuesto IVA en el módulo de ventas del sistema.	Incumplimiento fiscal del art. 162 inciso segundo del Código Tributario.
3.5	Registro de Eventos	La bitácora del sistema tiene un tiempo máximo de almacenamiento de dos meses.	Incapacidad de rastrear transacciones y/o modificaciones a datos, clientes., partidas cuentas y de prevenir/corregir riesgos de fraude.
3.7.1	Procesos de negocio relacionados y	Los puntos de venta de kioscos no han sido	Negocio en marcha incierta, suspensión o cierre del negocio.

REF.	ÁREA	DEBILIDADES DEL CONTROL INTERNO	RIESGOS IDENTIFICADOS
	cumplimiento de obligaciones legales	autorizados por la administración tributaria	
3.7.2	Procesos de negocio relacionados y cumplimiento de obligaciones legales	El sistema no permite incorporar en las transacciones las retenciones y percepciones del impuesto IVA	Imposición de multas por la administración Tributaria por incumplimiento fiscal del Art. 162 inciso segundo del Código Tributario.
3.7.2	Procesos de negocio relacionados y cumplimiento de obligaciones legales	Los reportes de movimientos y existencias del inventario no están de conformidad a los requerimientos de la administración tributaria	Imposición de multas por la administración Tributaria por incumplimiento fiscal del Art. 142 inciso segundo del Código Tributario
ACTIVIDADES DE CONTROL			
4.1.1	Seguridad de accesos	El personal de TI tiene la posibilidad de obtener accesos más allá de los necesarios para realizar sus tareas	La posibilidad de que el personal de informática obtenga permisos de acceso más allá de los necesarios para realizar sus tareas, dejando así de funcionar la segregación de funciones.
4.1.1	Seguridad de accesos	No existe una gestión de usuarios con privilegios especiales	Accesos no autorizados a los datos clave que pueden tener como resultado la destrucción o cambios indebidos de los mismos, incluido el registro de transacciones no autorizadas o inexistentes, o un registro inexacto de las transacciones.
4.1.2	Cambios en los programas	No existe una comprobación de saldos al momento de cambiar un sistema contable informático	Inconsistencia de datos entre el sistema anterior y el sistema nuevo.
4.2.1	Origen de datos	Ausencia de formularios físicos para documentar el origen e inicio de las transacciones	Registro de transacciones no autorizadas, inexistentes o sin respaldo.
4.2.1	Origen de datos	Los datos no son contabilizados al momento en que ocurren las transacciones	Carencia de información oportuna, disponible y exacta de la información.

REF.	ÁREA	DEBILIDADES DEL CONTROL INTERNO	RIESGOS IDENTIFICADOS
4.2.3	Proceso de datos	Ausencia de procedimientos para la verificación de la integridad y consistencia de la información almacenada en el sistema de recargas	Imposibilidad para detectar errores en los montos de ventas, inventario y costo de ventas
4.2.3	Proceso de datos	Falta de procedimientos para verificar los saldos del periodo anterior con respecto a los saldos del periodo actual	Inconsistencia de saldos iniciales del periodo actual.
4.2.4	Salida de datos	Los reportes generados por el sistema no permiten tomar decisiones empresariales, debido a que necesitan ser reformateados.	Carencia de información oportuna, disponible y exacta de la información, intervención manual inadecuada.
SEGUIMIENTO DE LOS CONTROLES			
5.1.2	Supervisar el control interno	Las evaluaciones del control interno TI son realizadas únicamente por personal de la entidad.	Revisiones con bajo nivel de objetividad, credibilidad, calidad, e independencia.
5.1.2	Supervisar el control interno	El sistema de control interno no es actualizado cuando surgen cambios en los riesgos.	No se realizan cambios necesarios en el control interno según los cambios en el riesgo. Obsolescencia desactualización de los controles.
5.1.2	Supervisar el control interno	No existe enfoque para la mejora continua del control interno.	Reducción progresiva de la efectividad de los controles.
5.1.3	Revisar la efectividad de los controles sobre los procesos del negocio	La organización no conoce los riesgos de tecnología relevantes a los procesos del negocio	Respuestas inapropiadas o nulas de las partes interesadas(gerente de TI, accionistas o junta directiva) ante los riesgos detectados

Fuente: elaboración propia.

Con esta información los auditores conocer puntualmente cada uno de los riesgos informáticos a los que se expone la entidad Recarga Directa, S.A. de C.V.; como siguiente paso se describirá la forma en que ellos deben de valorarlos.

3.3.4 Paso 4: valoración de los riesgos, matriz de riesgos y respuestas globales de auditor.

Descripción general de la matriz de riesgo.

Se trata de un esquema que relaciona los riesgos identificados, resultantes de las debilidades del control, con una serie de elementos que le permitirán al auditor de estados financieros determinar un enfoque global de auditoria, así como los procedimientos de control necesarios.

Riesgos identificados

En esa columna se detalla puntualmente el riesgo que a juicio del auditor, ha podido encontrar como parte de la naturaleza de la entidad y las debilidades del control interno TI (Ver tabla No. 15).

¿Qué podría estar equivocado?

Expresa precisamente cuales clases específicas de transacciones y/o saldos de cuentas podrían afectarse en caso de que el riesgo se materializara. En este apartado es valorado cada riesgo con el posible impacto a nivel de:

- Estados financieros de forma global.
- A nivel de aseveraciones, clases de transacciones o cuentas.

Al respecto la normativa establece:

"Los riesgos generalizados a menudo se derivan de un débil ambiente de control interno y afectan potencialmente muchas áreas, revelaciones y aserciones del estado financiero. Esos riesgos probablemente afectarán la valoración del riesgo a nivel de estado financiero y requerirán una respuesta general tal como más trabajo de auditoría, asignación de personal más experimentado, por parte del auditor". (IFAC, Auditoria Financiera de PYMES, 2007, p. 150.)

Aseveraciones:

Para identificar el tipo de aseveración se han establecido de conformidad a la NIA 315.A112 y están representados por los literales siguientes:

A. Afirmaciones sobre tipos de transacciones y hechos durante el periodo objeto de auditoría.
B. Sobre saldos contables al cierre del periodo.
C. Sobre la presentación e información a revelar.

Para efectos de referenciar los cuestionarios y la matriz hemos clasificado las aseveraciones de la manera siguiente:

Tabla 16. Abreviatura de las aseveraciones.

Abreviaciones	Aseveraciones	Concepto
O	Ocurrencia	Los hechos, transacciones y otras cuestiones revelados han ocurrido y corresponden a la entidad.
E	Exactitud	Las cantidades y otros datos relativos a las transacciones y hechos se han registrado adecuadamente y se muestran fielmente.
Ex	Existencia	Los activos, pasivos y el patrimonio neto existen.
I	Integridad	Se han registrado y revelado todos los hechos y transacciones que tenían que registrarse e incluirse en los estados financieros.
D	Derechos y obligaciones legales	La entidad posee o controla los derechos de los activos, y los pasivos son obligaciones de la entidad.
V	Valoración	Los activos, pasivos y el patrimonio neto figuran en los estados financieros por importes apropiados y cualquier ajuste de valoración o imputación resultante ha sido adecuadamente registrado.
C	Clasificación y Comprensibilidad	La información financiera se presenta y describe adecuadamente, y la información a revelar se expresa con claridad.
Co	Corte	Las transacciones y los hechos se han registrado en el periodo correcto.

Fuente: elaboración propia.

Valoración del riesgo.

Después de identificar los riesgos y los tipos de declaración equivocada contenidos en los estados financieros que pudieran ocurrir, el siguiente paso es valorar o clasificar su significancia. Esto se logra a través de la determinación de:

- **Probabilidad de ocurrencia del riesgo (P)**

Es considerada evaluar la probabilidad asignando un puntaje numérico del 1 a 5, a más alto el puntaje, más probable que el riesgo ocurrirá. Sin embargo el auditor en el uso de su juicio profesional puede clasificarlo como probabilidad alta, media o baja.

- **Impacto monetario de la ocurrencia del riesgo (I)**

Es considerado evaluar el impacto asignando un puntaje numérico del 1 a 5, a más alto el puntaje, más impacto tendrá el riesgo. Sin embargo el auditor en el uso de su juicio profesional puede clasificarlo como impacto alto, medio o bajo.

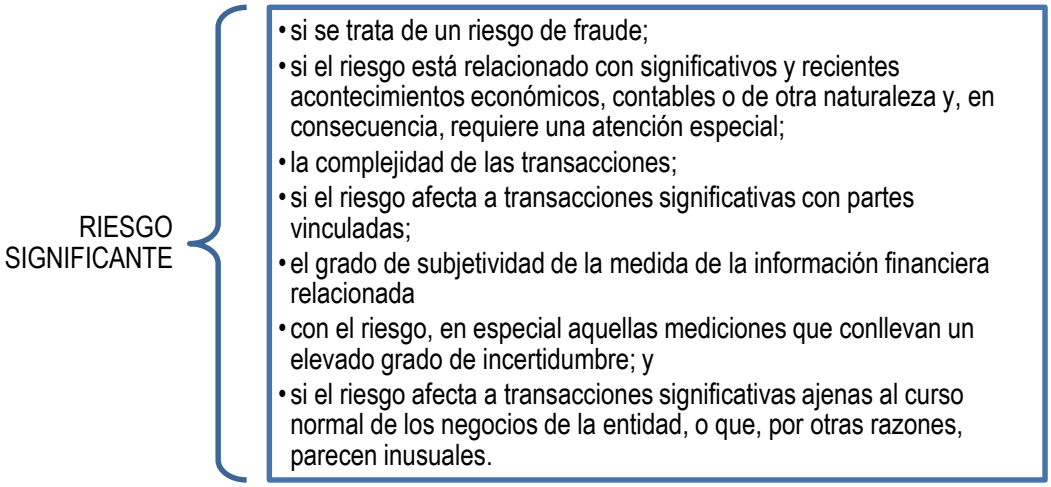
Riesgo combinado o riesgo total (RC)

Los puntajes numéricos para la probabilidad y el impacto se multiplican para dar un puntaje combinado o general.

Riesgo significante.

Este apartado se refiere a la alta posibilidad que ocurra un error de importancia identificado, que por tal motivo afectaría a los estados financieros en forma significativa, un riesgo es importante de acuerdo a la NIA 315.27.

Figura 11. Factores para determinación de riesgos significantes.



Fuente: IFAC, NIA 315 "Identificación y valoración de los riesgos de incorrección material mediante el conocimiento de la entidad y de su entorno", 2011, apartado 27.

Enfoque global de auditoría.

En esta parte el auditor diseña e implementa respuestas globales para responder al riesgo valorado anteriormente.

Procedimientos de auditoría.

Finalmente es planteado un procedimiento básico que permite identificar el impacto del riesgo resultante en la información financiera que es auditada, de este modo, el auditor comprenderá no solamente una estimación del posible impacto, sino que también puede determinar a través del uso de procedimientos analíticos la medición real de los efectos de la materialización del riesgo.

Tabla 17. Matriz de riesgos.

IMPACTO EN LAS VALORACIONES	RIESGOS IDENTIFICADOS	¿QUÉ PODRÍA ESTAR EQUIVOCADO?	ASEVE-RACIONES	VALORACIÓN DEL RIESGO			RIESGO SIGNIFICANTE	ENFOQUE GLOBAL DE AUDITORÍA	PROCEDIMIENTOS DE AUDITORÍA
				P	I	RC			
A NIVEL DE ESTADOS FINANCIEROS	A Pobre actitud de la administración hacia los controles, resistencia al cambio del entorno de TI, dependencias de tecnología en una sola persona Ambiente de control	Ineficacia del diseño, administración y seguimiento de los controles.	Todas	2	4	8	S	Recalcar al equipo de auditoría la necesidad de mantener el escepticismo profesional.	Ampliar el conocimiento sobre la actuación de la administración. Verificar en qué manera la administración puede eludir los controles. Indagar sobre el cumplimiento de leyes y regulaciones respecto a la información confidencial de sus clientes.
A NIVEL DE ESTADOS FINANCIEROS	B Falta de un modelo de valorización de riesgos de TI por parte de la entidad y su impacto en la información financiera que da como resultado respuestas inadecuadas para aceptar, reducir, mitigar el riesgo. Proceso de valorización del riesgo por la entidad.	Principio de negocio en marcha	Todas	2	5	10	S	Asignar empleados con mayor experiencia y con cualificaciones específicas o amplias de TI. Incorporar elementos adicionales de imprevisibilidad en la selección de los procedimientos de auditoría posteriores que se vayan a realizar.	Valorar junto con la administración de la entidad, los posibles riesgos Ampliación de pruebas de detalle y sustantivas.
A NIVEL DE SALDOS,	C	**Gastos**	V, E	5	5	25	S	Asignar recurso humano adicional	Reprocesamiento manual de la depreciación.

IMPACTO EN LAS VALORACIONES	RIESGOS IDENTIFICADOS	¿QUÉ PODRÍA ESTAR EQUIVOCADO?	ASEVE-RACIONES	VALORACIÓN DEL RIESGO			RIESGO SIGNIFICANTE	ENFOQUE GLOBAL DE AUDITORÍA	PROCEDIMIENTOS DE AUDITORÍA
				P	I	RC			
CUENTAS Y TRANSACCIONES	Inconsistencia entre las políticas contables de las depreciaciones y amortizaciones versus los valores parametrizados en el sistema. Sistema de información y comunicación	- Depreciación **Propiedad, Planta y Equipo** - Depreciación Acumulada							
A NIVEL DE SALDOS, CUENTAS Y TRANSACCIONES	D Inadecuada valuación de las estimaciones de incobrabilidad cuentas por cobrar por parte del sistema. Valores parametrizables	**Cuentas por Cobrar comerciales.** - Estimaciones de incobrabilidad de cuentas por cobrar	V, E	3	4	12	S	Asignar recurso humano adicional	Revisar las políticas de incobrabilidad, incluyendo el registro histórico de la entidad.
A NIVEL DE ESTADOS FINANCIEROS	E Diseño inadecuado del sistema Imposición de multas por la administración Tributaria por incumplimiento fiscal de los arts. 162 inciso segundo y 142 del Código Tributario.	Incumplimiento de leyes y regulaciones	Todas	5	4	20	S	Indagar sobre otros posibles incumplimientos fiscales del sistema	Preparar un marco de trabajo sobre las obligaciones fiscales e la empresa versus las opciones disponibles del sistema.

IMPACTO EN LAS VALORACIONES	RIESGOS IDENTIFICADOS	¿QUÉ PODRÍA ESTAR EQUIVOCADO?	ASEVE-RACIONES	VALORACIÓN DEL RIESGO			RIESGO SIGNIFICANTE	ENFOQUE GLOBAL DE AUDITORÍA	PROCEDIMIENTOS DE AUDITORÍA
				P	I	RC			
A NIVEL DE ESTADOS FINANCIEROS	F La posibilidad de que el personal del departamento de TI obtenga permisos de acceso más allá de los necesarios para realizar sus tareas, dejando así de funcionar la segregación de funciones. Controles Generales y de aplicación	Accesos no autorizados a los datos que pueden tener como resultado la destrucción de datos o cambios indebidos de los mismos, incluido el registro de transacciones no autorizadas o inexistentes, o un registro inexacto de las transacciones.	Todas	2	5	10	S	Revisión de los perfiles de acceso del departamento de TI. Necesidad de requerir con un experto para revisión de bitácora en la base de datos del sistema	Indagar en la bitácora del sistema las transacciones realizadas por usuarios distintos a los autorizados. Revisión detallada de los perfiles de usuario asignados los miembros de TI.
A NIVEL DE ESTADOS FINANCIEROS	G La bitácora o registro de eventos del sistema, permite almacenar un máximo de dos meses de histórico de modificación, adición y eliminación de transacciones.	Incapacidad para responsabilizar o individualizar la fuente de las transacciones.	Todas	2	4	8	S	Debido al anonimato de las transacciones Revisar aquellas que llamen la atención, como liquidación de saldos de cuentas por cobrar, préstamos a empleados, movimientos de caja, etc.	Realizar visitas periódicas a la empresa y en cada una solicitar las pistas de auditoría. Mantener el escepticismo profesional debido al anonimato en la ocurrencia de las transacciones. Aumentar el tamaño de la muestra y corroborar el origen de las transacciones.
A NIVEL DE SALDOS, CUENTAS Y TRANSACCIONES	H Imposibilidad para detectar errores en los montos de ventas,	**Ingresos** Ventas de recargas no reconocidas **Gastos**	V, E, Ex, I	3	2	6	S	Revisión de las recargas realizadas en un periodo determinado.	Realizar conciliaciones entre las recargas realizadas y las bajas en inventarios. Realizar comparación entre recargas disponibles para la venta y los saldos de inventarios a una fecha determinada.

IMPACTO EN LAS VALORACIONES	RIESGOS IDENTIFICADOS	¿QUÉ PODRÍA ESTAR EQUIVOCADO?	ASEVE-RACIONES	VALORACIÓN DEL RIESGO			RIESGO SIGNIFICANTE	ENFOQUE GLOBAL DE AUDITORÍA	PROCEDIMIENTOS DE AUDITORÍA
				P	I	RC			
	inventario y costo de ventas	Costo de ventas no reconocidas **Inventarios** Saldos incorrectos de recargas disponibles para la venta						Análisis estadístico de los costos de venta por recargas. Revisión del kardex.	
A NIVEL DE SALDOS, CUENTAS Y TRANSACCIONES	I Registro de transacciones no autorizadas, inexistentes o sin respaldo.	**Efectivo y equivalentes** Efectivo inexistente en los kioscos **Ingresos** Ventas de recargas en exceso	E	5	3	15	S	Revisión del saldo de efectivo administrado por cada kiosco. Inspección técnica de los sensores de reconocimiento de valores monetarios.	Efectuar cortes de caja y comparar los resultados con el efectivo manejado contablemente por el kiosco. Realizar una transacción de recarga de prueba, utilizando todos las denominaciones monetarias permitidas por el kiosco.

Fuente: elaboración propia

EJEMPLO SOBRE LA FORMA DE COMPLETAR LA MATRIZ DE RIESGO, TOMANDO EL LITERAL "C".

Para describir cada uno de estos elementos intervinientes en la matriz se explica a continuación el riesgo identificado "C", Así:

- **Riesgos identificados**

  Para el caso seleccionado se describe textualmente el riesgo: "**inconsistencia entre las políticas contables de las depreciaciones y amortizaciones versus los valores parametrizados en el sistema por parte de la empresa**". Este proviene de las indagaciones ante la administración mediante el cuestionario y la observación e inspección.

- **¿Qué podría estar equivocado?**

  Una inconsistencia entre las políticas contables establecidas para las depreciaciones se traduciría en un gasto por depreciación sobre-valorado o sub-valorado, así mismo, el valor en libros de la propiedad planta y equipo puede presentar un valor incorrecto. Por ejemplo si la sociedad establece políticas de depreciación para la partida de equipo de cómputo en un 20% anual, el sistema sin embargo está configurado para procesar un porcentaje de 50%, existe una diferencia entre la política contable escrita y la aplicada que da lugar a equivocaciones.

- **Aseveraciones.**

  Continuando con el ejemplo de riesgo, se afirma que al existir un gasto por depreciación y valor en libros de los activos en forma errónea, el valor de las partidas registradas durante el periodo es incorrecto, así también el gasto esta expresado por un valor inadecuado, por lo que las aseveraciones están impactadas de la forma siguiente: "E" de exactitud y "V" de valoración, el valor en libros de los activos puede estar registrado de forma inadecuada y por importes incorrectos.

  Cuando no se puede aplicar a una cuenta en particular el impacto es en los estados financieros a nivel global y está relacionado con todas las aseveraciones.

- **Valoración del Riesgo.**

  A juicio del equipo de auditores, se establece el valor “5” como la probabilidad establecida al riesgo, debido a que el error de contabilización del gasto por depreciación, el sistema lo realiza de forma automática y recurrente durante cada mes. El valor del impacto se establece en “5”, en razón de la significancia de la propiedad, planta y equipo en los activos totales.

- **Riesgo Significante.**

  De acuerdo al caso planteado se estableció que el riesgo en mención es de carácter significante (S), así como el resto de riesgos subsecuentes.

- **Enfoque global de auditoría.**

  En cuanto al tema en cuestión, debido a que el riesgo es significativo se ha establecido uno de los enfoques que establece la NIA 330.A1 manifestando que: “se debe asignar empleados con mayor experiencia o con cualificaciones específicas”.

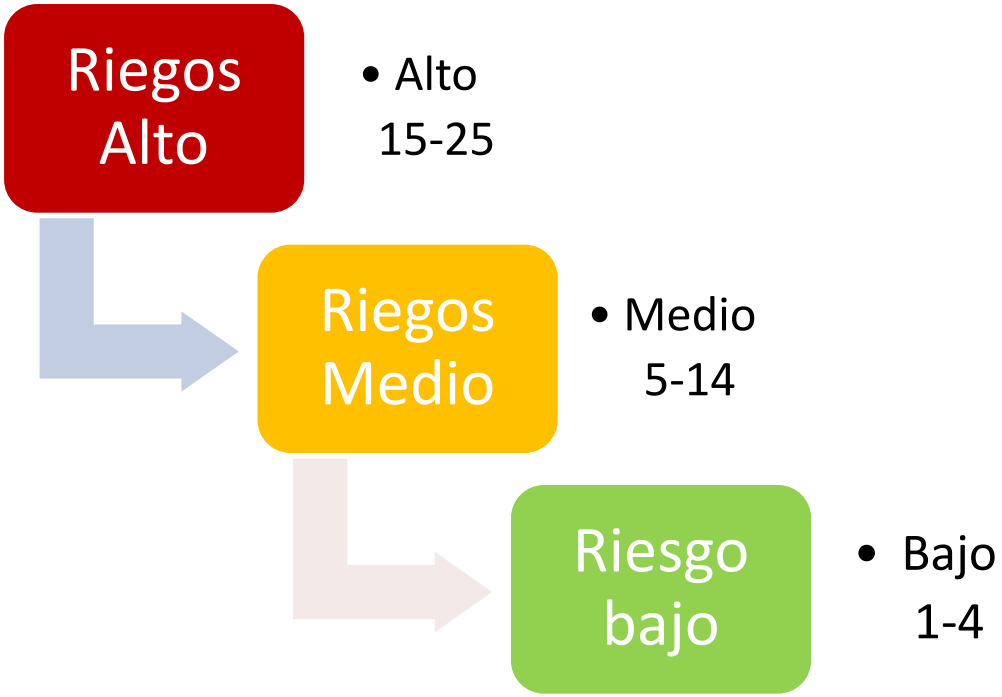
- **Procedimientos de auditoría.**

  El riesgo seleccionado concluye con el procedimiento siguiente: reprocesamiento manual de la depreciación.

MAPA DE CALOR

En base a los puntajes de probabilidad multiplicada por impacto para cada riesgo, establecemos la manera de graficar la criticidad de acuerdo a la siguiente figura.

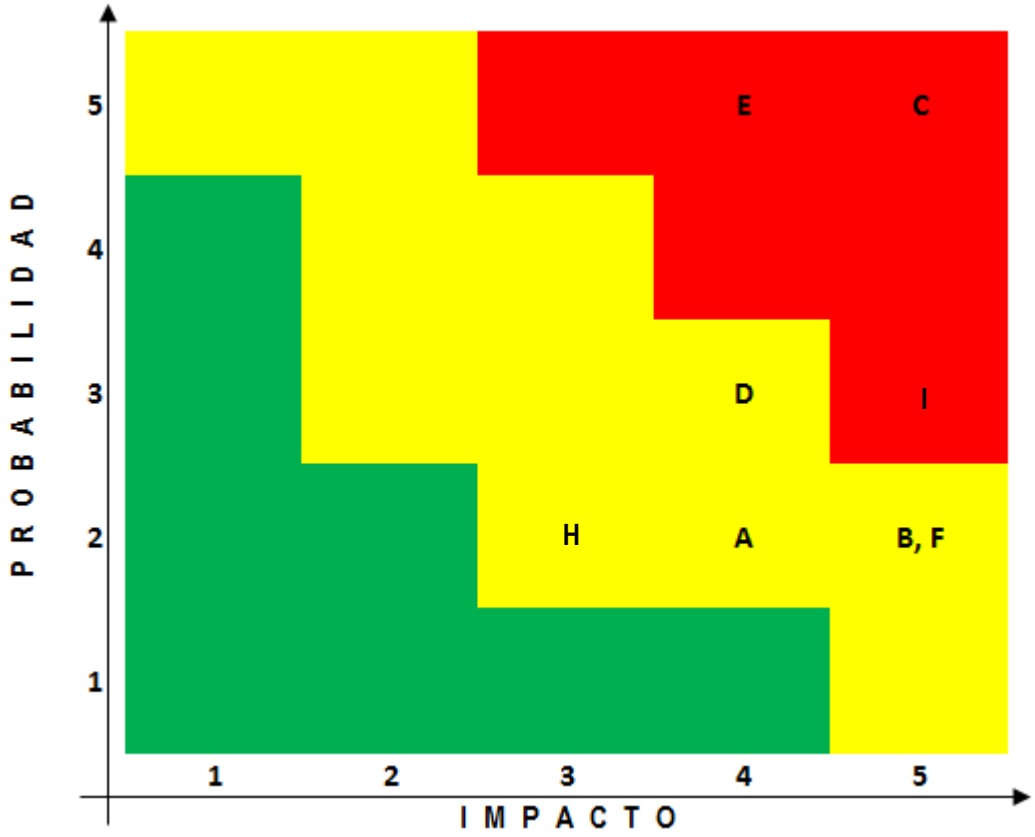
Figura 12. Niveles de criticidad de la probabilidad por el impacto.



Fuente: elaboración propia.

De los riesgos detallados en la tabla anterior, se procede a graficar para tener un panorama más claro de los principales, que requieren atención del auditor.

Figura 13. Mapa de riesgos.



Fuente: elaboración propia.

Se puede apreciar que los riesgos que requieren consideración principal, son los contenidos en los literales “C”, “E” e “I”, relacionados con los gastos, propiedad, planta y equipo, el incumplimiento de leyes y regulaciones y con el registro de los ingresos y el efectivo.

CAPITULO IV: CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

En la actualidad existe una creciente dependencia de la tecnología de información y comunicación (TIC´s) en las diferentes entidades auditadas por las firmas de auditoría, debido a que en algún grado sus sistemas de información y procesos de negocio se encuentran automatizados.

Como parte del proceso de evaluación del control interno informático que la normativa internacional exige a los auditores, las firmas comúnmente basan su enfoque en aspectos tradicionales y en la emisión de resultados (reportes) o salida de información por parte de los sistemas, dejando de verificar otros aspectos importantes como la entrada, procesamiento de datos, seguridad (física y lógica) en los sistemas y en muchas ocasiones se ven en la necesidad de auxiliarse de un experto para evaluar dichos aspectos.

Generalmente las firmas de auditoría presentan en su equipo de trabajo poca o nula capacitación sobre aspectos relacionados al área de tecnologías de información.

Los mayores riesgos con los que se encuentran los auditores en el proceso de evaluación de control interno relevante a la información financiera son la mala aplicación de políticas contables y la integridad de los datos debido a que los usuarios se adaptan a los sistemas y no lo contrario.

Las firmas se ven en dificultades al momento de ejecutar una evaluación de control interno informático relevante a la información financiera conforme a normativa debido a que el material con el que cuentan es insuficiente.

4.2 Recomendaciones

Ante la creciente dependencia de TI que están sufriendo los negocios en la actualidad, se recomienda al auditor a estar alerta ante esta situación y ya no realizar evaluaciones sólo a papeles físicos sino también a información electrónica.

Se recomienda a las firmas incluir en los memorándums de planeación de auditoría financiera las áreas relacionadas a la identificación y evaluación del control interno de TI relevante a la información financiera con el fin de minimizar su riesgo y considerarlo en la naturaleza, oportunidad y extensión de sus procedimientos.

IFAC exige a los países miembros a través de la Declaración Sobre las Prácticas Internacionales de Formación No. 2 (IEPS2) titulada "Tecnologías de Información para Contadores Profesionales" tener conocimientos adecuados en el área informática; en este sentido, se recomienda a los gremios comprometidos con la profesión de contaduría pública y auditoría impartir seminarios y capacitaciones para mejorar las competencias que dicha normativa establece.

Asimismo se recomienda a las firmas que implementen un programa de auto capacitación sobre temas relevantes al área de informática para así incrementar la competencia de su personal y dar cumplimiento a exigencias de normativa internacional en el desarrollo de encargos de auditoría.

Comprobado que las firmas poseen dificultades al momento de ejecutar una evaluación de control interno a las tecnologías de información; se recomienda hacer uso de la presente metodología, la cual detalla la forma de cómo identificar y evaluar riegos de TI cuando la información financiera se encuentra bajo un ambiente de sistemas computarizados.

BIBLIOGRAFÍA

Alvarenga Mendoza, Elber Alexander; Hernández Villanueva, Maira Roxana; León Deras, Javier Atilio. (2006). "*Guía práctica para obtener evidencia de auditoría en un ambiente de sistemas de información por computadora SIC, para pequeñas y medianas firmas de auditoría en El Salvador"*. Tesis de Licenciatura en Contaduría Pública, Facultad de Ciencias Económicas, Universidad de El Salvador, El Salvador.

Alvin A. Arens, Randal J. Elder, Mark S. Beasley. (2007). "*Auditoría un Enfoque Integral."* Decimoprimera edición. Estado de México, México. Pearson Educación de México, S.A. de C.V., Prentice-Hall.

Asociación de Auditoría y Control de Sistemas de Información (ISACA siglas en inglés)**.** (2012)**. "**Marco de Negocio para el Gobierno y la Gestión de TI en la Empresa COBIT 5**".** Illinois, Estados Unidos (traducido al español desde la versión en inglés de COBIT 5 por el Capítulo de Madrid de ISACA)

- **Consejo Normativo de la Asociación de Auditoría y Control de Sistemas de Información.** (2005). *"Normas Generales para la Auditoría de Sistemas de Información (NAS)".*

Código Tributario

D.L. No. 230, del 14 de diciembre de 2000, publicado en el D.O. No. 241, tomo 349, del 22 de diciembre de 2000.

Ultima reforma:

D.L. No. 958 de fecha 14 de diciembre de 2011, publicado en el D.O. No. 235, Tomo 393 de fecha 15 de diciembre de 2011.

Chinchilla Flamenco, Dionisio Abraham. (2007). *"Guía didáctica I para seminarios de investigación social".* (Primera edición). San Salvador. El Salvador. Ediciones Chinchilla. Impreso por Talleres Gráficos UCA.

Consejo de Vigilancia de la Profesión de Contaduría Pública. (2003). *"Norma de Educación Continuada".* Gobierno de El Salvador. Disponible en www.consejodevigilancia.gob.sv/. Consultado en abril 2013.

- *"Listado de personas naturales y jurídicas autorizadas para ejercer la Contaduría Pública y Auditoría al 31 de diciembre del 2012".* Gobierno de El Salvador. Disponible en www.consejodevigilancia.gob.sv/. Consultado en abril 2013.

Cornejo Pérez, Mario Hernán. (2008). "*Tecnología de información en el contexto profesional del contador público*", Revista Ábaco Contable No. 2. Escuela de Contaduría Pública. Facultad de Ciencias Económicas. Universidad de El Salvador.

Federación Internacional de Contadores (IFAC). "*Normas Internacionales de Auditoría y Control de Calidad (NIA´S)",* edición 2011. Reino Unido.

- **Consejo de Normas Internacionales de Formación en Contaduría**. *"Manual de los Pronunciamientos Internacionales de Formación"* Normas Internacionales de Formación (IES), edición 2008. Reino Unido.
- **Consejo de Normas Internacionales de Formación en Contaduría**. Declaración Internacional de Práctica de Auditoría, *"Tecnología de Información para Contadores Profesionales", (IEPS 2), edición 2007.* Reino Unido.

Hernández Sampieri, Roberto; Fernández Collado, Carlos; Baptista Lucio, Pilar. (2003). "*Metodología de la Investigación"*, (3ª Edición). México. Editorial Mc Graw Hill Interamericana.

Malbernat, Lucía Rosario. "*Tecnologías educativas e innovación en la Universidad"* http://www.lacapitalmdp.com/noticias/La-Ciudad/2010/12/27/168009.htm, consultado el 12 de junio del 2013.

Muñoz Razo, Carlos. (2011). *"Cómo elaborar y asesorar una investigación de tesis"* (Segunda edición). Estado de México. México. Pearson Educación de México, S.A. de C.V. Prentice-Hall

- *"Auditoría en Sistemas Computacionales"* (Primera edición 2002). Estado de México. México. Pearson Educación de México, S.A. de C.V. Prentice-Hall

Velthius Mario Piattini, Navarro Emilio del Peso, Ruiz Mar del Peso (2008). "*Auditoría de Tecnología y Sistemas de Información". Madrid, España. RA-MA Editorial.*

ANEXOS

ÍNDICE DE ANEXOS

ANEXO 1

Listado de firmas de auditoría (personas jurídicas) autorizadas por el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría (CVPCPA)[9]

PERSONAS JURIDICAS QUE HAN ACTUALIZADO INFORMACION DEL REGISTRO AL 28 DE ENERO DE 2013

2572	A. BLANCO Y ASOCIADOS
1930	A.B. DE OSNEROS Y COMPAÑÍA
3825	ACC, ASOCIADOS, S.A. DE C.V.
2042	ADAN HENRIQUEZ VALLE Y ASOCIADOS
4431	ADVISERS AUDIT & ACCOUNTING, S.A. DE C.V.
3183	AFE INTERNACIONAL, S.A. DE C.V.
4268	AGUILAR SANTOS, S.A. DE C.V.
2620	AGUILAR, FLORES Y ASOCIADOS
2301	AGUILERA Y ASOCIADOS
1988	AGUIÑADA Y ASOCIADOS, S.A. DE C.V.
2571	ALAS HERNANDEZ Y ASOCIADOS
2180	ALAS LINARES Y ASOCIADOS
3944	ALFARO MENDOZA, S.A. DE C.V.
1514	ALVAREZ FLORES Y COMPAÑÍA
4212	AMAYA & GUEVARA AUDITORES, S.A. DE C.V.
0786	ANAYA VILLEDA Y ASOCIADOS
4410	ANDRADE PORTILLO, S.A. DE C.V.
2167	ARANIVA GARCIA ASOCIADOS
2424	AREVALO PINTO Y COMPAÑÍA
2404	AREVALO, ALLEN Y ASOCIADOS
1583	ARTEAGA ARGUMEDO Y ASOCIADOS
3672	ASESORIA Y CONSULTORIA DE NEGOCIOS, S.A. DE C.V.
4215	AUDIT & TAX SERVICES, S.A. DE C.V.
4289	AUDITORES AUTORIZADOS, WEDS & COMPAÑIA, S.A. DE C.V.
1326	AUDITORES Y ASESORES, S.A. DE C.V.
3798	AUDITORES Y CONSULTORES CORPORATIVOS, S.A. DE C.V.
3614	AUDITORES Y CONSULTORES DE NEGOCIOS, S.A. DE C.V.
3656	AUDITORES Y CONSULTORES SALVADOREÑOS, S.A. DE C.V.
4138	AUDITORES Y CONTADORES, S.A. DE C.V.
4236	AUDITORES, CONSULTORES CASTRO ARANO, S.A. DE C.V.
4252	AUDITORES, CONSULTORES Y CONTADORES, S.A. DE C.V
3675	AUDITORIA Y CONSULTORIA ESTRATEGICA, S.A. DE C.V.
4141	AUDITORIA Y SERVICIOS DE CONSULTORIA, S.A. DE C.V.
4400	AVALOS, CARDONA & ASOCIADOS, S.A. DE C.V.
4143	AVELAR & ASOCIADOS, S.A. DE C.V.
3673	AVELAR PLEITEZ, S.A. DE C.V.
2730	BARAHONA & BENITEZ ASOCIADOS
3571	BARAHONA & CARCAMO AUDITORES ASOCIADOS, LIMITADA DE C.V.
2505	BARAHONA HENRIQUEZ Y ASOCIADOS
3809	BARAHONA HUEZO Y ASOCIADOS, S.A. DE C.V.
2859	BARAHONA VARGAS ASOCIADOS
1089	BENJAMIN WILFRIDO NAVARRETE Y CIA
3008	BLANCO URQUIA Y ASOCIADOS
3457	BMM & ASOCIADOS, S.A. DE C.V.
1327	BONILLA MUÑOZ Y ASOCIADOS
3921	BUCARO JOVEL & ASOCIADOS, S.A. DE C.V.
2857	CABRERA MARTINEZ, S.A. DE C.V.
0382	CALDERON MENJIVAR Y ASOCIADOS
4216	CAÑENGUEZ & CAÑENGUEZ, S.A. DE C.V.
1898	CARLOS ALBERTO MEJIA VALLE Y ASOCIADOS
2565	CARRANZA Y CARRANZA Y ASOCIADOS
3354	CASTELLANOS CHACON, LTDA. DE C.V.
2679	CASTELLANOS GOMEZ Y ASOCIADOS
3532	CASTELLANOS, GOMEZ, CABRERA Y ASOCIADOS, S.A. DE C.V.
3321	CASTILLO GUZMAN AUDITORES Y CONSULTORES, S.A. DE C.V.
3006	CCA AUDITORES Y CONSULTORES ASOCIADOS, S.A. DE C.V.
0665	CERRITOS CERRITOS Y COMPAÑÍA
3488	CHAVEZ QUEVEDO Y ASOCIADOS
2504	CHICAS ALFARO Y ASOCIADOS
0300	CISNEROS, CASTRO Y CIA
1880	CIUDAD REAL Y ASOCIADOS, S.A. DE C.V.
3637	COCAR ROMANO Y COMPAÑÍA
3353	CONSULTORES AUDITORES MORALES IGLESIAS, S.A. DE C.V.
2944	CONSULTORES PROFESIONALES TRIBUTARIOS, S.A. DE C.V.
3992	CONTADORES NAJARRO Y COMPAÑÍA
2934	CONTADORES PUBLICOS ASOCIADOS, S.A. DE C.V.
4183	CONTADORES PUBLICOS AUDITORES, S.A. DE C.V.
3920	CONTADORES PUBLICOS QUINTANILLA & CIA., S.A. DE C.V.
4249	CONTADORES Y AUDITORES RIVAS & ASOCIADOS, S.A. DE C.V.
3287	CORNEJO & UMAÑA, LIMITADA DE CAPITAL VARIABLE
0714	CORPEÑO Y ASOCIADOS
3288	CRUZ CHAVEZ & COMPAÑÍA
3205	DAMAS COCAR Y COMPAÑÍA
1557	DESPACHO DE AUDITORIA AMAYA PINEDA Y ASOCIADOS
4144	DESPACHO VASQUEZ Y ASOCIADOS LTDA. DE C.V.
2497	DIAZ MARTINEZ Y ASOCIADOS
3732	DTT EL SALVADOR, S.A. DE C.V.
2856	DURAN PONCE Y COMPAÑÍA
2858	EBARRIENTOS Y ASOCIADOS, S.A. DE C.V.
0859	ELIAS & ASOCIADOS
2621	ESCALANTE-ESCALANTE Y COMPAÑÍA
3419	ESCOBAR, ORTIZ, GUARDADO, S.A. DE C.V.
0425	FERNANDEZ Y FERNANDEZ ASOCIADOS
0215	FIGUEROA JIMENEZ & CO., S.A.
0259	FIGUEROA JIMENEZ Y ASOCIADOS
4073	FLORES FLORES Y ASOCIADOS, S.A. DE C.V.
3572	FLORES FUNES & COMPAÑÍA
4188	FLORES GUADRON Y ASOCIADOS, S.A. DE C.V.
0267	FREDY S. CHICAS Y COMPAÑÍA
3007	GARCIA LAZO Y COMPAÑÍA
1232	GARCIA ROMERO Y ASOCIADOS
4142	GOCHEZ & ASOCIADOS-AUDITORES, CONSULTORES Y ASESORES, S.A. DE C.V.
2427	GOMEZ SANCHEZ Y COMPAÑÍA
3298	GONZALEZ BARAHONA ASOCIADOS, S.A. DE C.V.
4500	GONZALEZ PINEDA, S.A. DE C.V.
2570	GRANDE CHAVARRIA Y ASOCIADOS

11

[9] Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría, "Listado de personas naturales y jurídicas para ejercer la contaduría pública y auditoría", en La Prensa Gráfica, San Salvador, 28 de enero de 2013, pág. 11 y 12.

CVPCPA CONSEJO DE VIGILANCIA DE LA PROFESION DE CONTADURIA PUBLICA Y AUDITORIA

1513	GRANT THORNTON PEREZ MEJIA, NAVAS, S.A. DE C.V.
3235	GRUPO INTERNACIONAL DE CONSULTORIA DE EL SALVADOR, S.A. DE C.V.
2400	GUADALUPE RODRIGUEZ Y ASOCIADOS
4038	GUERRA PORTILLO CONSULTORES, S.A. DE C.V.
4146	GUEVARA FLAMENCO, S.A. DE C.V.
3556	GVM Y ASOCIADOS, S.A. DE C.V.
3674	HERNANDEZ CUEVAS & COMPAÑIA, DE C.V.
2681	HERNANDEZ GONZALEZ Y ASOCIADOS
2416	HERRERA ALAS Y ASOCIADOS
1264	HLB EL SALVADOR, S.A. DE C.V.
4526	HR CONSULTORES DE NEGOCIOS Y AUDITORES, S.A. DE C.V.
2507	HUMBERTO ANTONIO MOLINA Y COMPAÑIA
2104	J. CISNEROS Y COMPAÑIA
0325	J.H. VALIENTE Y ASOCIADOS
3824	JACOBO Y ASOCIADOS, S.A. DE C.V.
2300	JEREZ GONZALEZ Y ASOCIADOS
3289	JMB AUDITORES Y CONSULTORES, S.A. DE C.V.
4148	JOVEL PONCE Y COMPAÑIA
1390	JOVEL, JOVEL Y COMPAÑIA
1048	JULIO CESAR GARCIA LAZO Y CIA
0566	K.C. PUBLIC ACCOUNTING SERVICES, LTDA. DE C.V.
0422	KPMG, S.A.
3216	L.F. JOVEL Y COMPAÑIA
2103	LATIN AMERICAN AUDIT & TAX CORPORATE EL SALVADOR LTDA. DE C.V.
3933	LOPEZ & ESTLANDER, AUDITORES Y CONSULTORES LTDA. DE C.V.
4251	LOPEZ & LOPEZ AUDITORES Y CONSULTORES, S.A. DE C.V.
2210	LOPEZ GRANADINO, S.A DE C.V.
2897	LOPEZ GUERRERO Y ASOCIADOS
3196	LOPEZ Y ASOCIADOS LTDA. DE C.V.
2922	LOPEZ, SOLITO Y ASOCIADOS
1929	LUIS ALONSO CORNEJO Y ASOCIADOS
2070	MARIA GUADALUPE RIVERA Y COMPAÑIA
2499	MARTINEZ GARCIA Y COMPAÑIA
1986	MARTINEZ SOLANO ASOCIADOS
2502	MARTINEZ-GARCIA Y ASOCIADOS
1931	MAURICIO J. ORELLANA MIXCO Y ASOCIADOS
2567	MAYORGA ORTIZ Y COMPAÑIA
3799	MEJIA GOMEZ Y ASOCIADOS
2622	MEJIA HERNANDEZ Y COMPAÑIA
0430	MEJIA, AGUIRRE Y ASOCIADOS
2170	MELENDEZ Y MELENDEZ ASOCIADOS
3175	MEMBREÑO VASQUEZ Y ASOCIADOS
1930	MENA RODRIGUEZ Y ASOCIADOS
2675	MINERO LEMUS Y ASOCIADOS
3623	MN AUDITORES-CONSULTORES, S.A. DE C.V.
2087	MONROY Y ASOCIADOS
4411	MONTENEGRO ESCOBAR Y ASOCIADOS, SOCIEDAD ANONIMA DE CAPITAL VARIABLE
3906	MORALES PEREZ VARELA, S.A. DE C.V.
2568	MORALES PEREZ Y ASOCIADOS
0183	MORALES Y MORALES ASOCIADOS
1328	MORAN MENDEZ Y ASOCIADOS, S.A. DE C.V.
0175	MORENO, PORTILLO Y ASOCIADOS, S.A. DE C.V.
1306	MURCIA & MURCIA, S.A. DE C.V.
1771	NAVARRETE CAMPOS Y COMPAÑIA
0941	NAVARRO GUEVARA Y ASOCIADOS
2401	OCHOA BENITEZ ASOCIADOS, S.A. DE C.V
4438	OCHOA RAMOS, S.A. DE C.V.
2855	ORELLANA Y ASOCIADOS
2500	ORELLANA, MORAN, CHACON Y ASOCIADOS
0335	ORTEGA, CISNEROS, DOMINGUEZ Y CIA.
2425	OSCAR MORALES Y ASOCIADOS
2990	P.S. ALVARENGA Y ASOCIADOS
3686	PAREDES & PAREDES CONSULTORES, S.A. DE C.V.
1103	PARKER ECHEVERRIA Y ASOCIADOS
4145	PAVON ARIGUETA Y COMPAÑIA, LTDA. DE C.V.
2168	PEREIRA PEREIRA Y ASOCIADOS
3150	PEREZ PORTILLO Y ASOCIADOS
2788	PIMENTEL CARRANZA & ASOCIADOS
4288	PLUS AUDIT, S.A. DE C.V.
3797	Q. M. & ASOCIADOS, S.A. DE C.V.
2440	QUIJANO MORAN Y COMPAÑIA
3151	QUIJANO TOCHEZ Y ASOCIADOS
4471	R B M AUDITORES Y CONSULTORES, S.A. DE C.V.
2627	R. GALLARDO Y COMPAÑIA
4409	R.D.C. AUDITORES, S.A. DE C.V.
4150	RAMIREZ MURCIA, ASOCIADOS
2423	RAMOS ALVARADO Y ASOCIADOS
3456	RAMOS REYES Y COMPAÑIA
4149	RCC AUDITORES & CONSULTORES, S.A. DE C.V.
2406	RECINOS, RECINOS Y COMPAÑIA
0524	REYES, QUINTANILLA Y ASOCIADOS
4525	RIOS UMAÑA, S.A. DE C.V.
2402	RIVAS NUÑEZ Y ASOCIADOS, S.A. DE C.V.
2978	RIVERA PALMA ASOCIADOS
2626	RODRIGUEZ CABRERA Y ASOCIADOS
2506	ROJAS MENDEZ Y COMPAÑIA
2566	ROMERO MEZA Y COMPAÑIA
2896	ROMERO PORTILLO & ASOCIADOS, S.A. DE C.V.
2810	ROQUE Y ROQUE ASOCIADOS
3227	ROSALES CHITA Y ASOCIADOS
3698	S.Z. CONSULTORES, S.A. DE C.V.
3894	SALMERON AUDITORES, S.A. DE C.V.
3862	SANTAMARIA CANALES Y ASOCIADOS, S.A. DE C.V.
4139	SANTOS & LOPEZ CONSULTORES Y AUDITORES, S.A. DE C.V.
4250	SERVICIOS INTEGRALES DE CONTADURIA PUBLICA, S.A. DE C.V.
0071	SERVICIOS PROFESIONALES ASOCIADOS, MEJIA Y ALVARENGA
2935	SERVICIOS PROFESIONALES NAZARETH, S.A. DE C.V.
3379	SERVICIOS TECNICOS DE CONSULTORIA Y AUDITORIA, S.A. DE C.V.
3744	SERVICIOS TRIBUTARIOS Y ASESORIA FINANCIERA, S.A. DE C.V.
4300	SIGNATURE GROUP, S.A. DE C.V.
0892	TOCHEZ FERNANDEZ, LIMITADA
3945	TORRES, BONILLA & ASOCIADOS, S.A. DE C.V.
3653	TURCIOS HENRIQUEZ, S.A. DE C.V.
3025	VALENCIA ELIAS, S.A. DE C.V.
3676	VALIENTE Y ASOCIADOS
2435	VASQUEZ RETANA Y ASOCIADOS
3685	VASQUEZ SALAZAR Y ASOCIADOS, S.A. DE C.V.
2923	VASQUEZ VIERA Y ASOCIADOS
0075	VEGA LOPEZ Y COMPAÑIA
2677	VELASQUEZ GRANADOS Y COMPAÑIA
2086	VENTURA SOSA, S.A. DE C.V.
3655	VENTURA-AUDITORES Y ASOCIADOS
2169	VILANOVA Y ASOCIADOS
3763	VILLAFUERTE GARCIA Y ASOCIADOS, S.A. DE C.V.
3418	ZELAYA GAVIDIA AUDITORES, S.A. DE C.V.
4147	ZELAYA RIVAS Y COMPAÑIA, S.A. DE C.V.
2503	ZELAYA RIVAS, ASOCIADOS Y COMPAÑIA

PERSONAS JURIDICAS QUE NO HAN ACTUALIZADO INFORMACION DEL REGISTRO AL 28 DE ENERO DE 2013

1523	ABARCA GOMEZ Y ASOCIADOS
2501	AGUILAR Y ASOCIADOS
0299	AGUILAR Y MORALES ASOCIADOS
2179	ALAS TOBAR ASOCIADOS
0284	ALFONSO ZARATE Y COMPAÑIA
2569	ALVARENGA BURGOS Y ASOCIADOS
0309	ARIAS ARIAS Y CO. DE C.V.
4020	AUDITORIA INTEGRAL Y CONSULTORIA, S.A. DE C.V.
3772	AUDITORIA Y CONSULTORIA, S. A. DE C. V.
0796	BARAHONA, RODRIGUEZ, PORTILLO Y ASOCIADOS
2397	BLANCO GARCIA ASOCIADOS
2403	CALLES RICO Y ASOCIADOS
0074	CASTELLANOS, CEA CAMPOS Y COMPAÑIA
2573	CASTRO ANAYA Y COMPAÑIA
3149	CHACON RIVERA Y ASOCIADOS
0522	CHICAS VILCHEZ Y COMPAÑIA
3586	CHICAS VILCHEZ Y RUIZ, S.A. DE C.V.
4194	CHICAS, FUENTES, ORTIZ Y ASOCIADOS, S.A. DE C.V.
3531	CISNEROS, VELASQUEZ Y ASOCIADOS
4140	CONSULTORES Y AUDITORES INTEGRALES, S.A. DE C.V.
4184	CONSULTORIA, OUTSOURCING, AUDITORIA, S.A. DE C.V.
3024	COREAS RIVAS Y ROMERO ASOCIADOS
1555	DARIO BERNAL TORRES Y ASOCIADOS
2399	DIAZ ALAS, ASOCIADOS
0476	DIAZ, MENA, SANCHEZ Y COMPAÑIA
3412	ERNST &YOUNG, EL SALVADOR, S.A. DE C.V.
0890	ESCOBAR, DURAN Y COMPAÑIA
0773	ESQUIVEL Y ASOCIADOS
0303	ESQUIVEL Y ESQUIVEL, ASOCIADOS
3398	FERNANDEZ GUZMAN Y ASOCIADOS
0178	FERNANDEZ, MORALES Y NAVARRETE
1219	FERNANDEZ, SOLORZANO Y ASOCIADOS
2860	FERNANDO ROMERO Y ASOCIADOS
2729	FLORES ALAS ASOCIADOS
0432	GALICIA CEA Y ASOCIADOS
2678	GARCIA CUELLAR Y ASOCIADOS
3426	GARCIA LOPEZ Y COMPAÑIA, S.A.
3879	GARCIA MENDEZ Y ASOCIADOS
3790	GLOBAL AUDITORES Y CONSULTORES, S. A. DE C. V.
0170	GOMEZ AGUILAR MENJIVAR Y CIA
2441	GONZALEZ, CHAVARRIA Y ASOCIADOS
2405	GUEVARA, CHICAS, PALACIOS & ASOCIADOS
1222	GUTIERREZ GONZALEZ AUDITORES-CONSULTORES
0275	GUZMAN ELIAS Y ASOCIADOS
3548	GUZMAN RIVERA & ASOCIADOS
3292	H.S. CHACHAGUA, S.A. DE C.V.
1545	HERNANDEZ MARTINEZ Y ASOCIADOS
0683	HERNANDEZ RECINOS Y COMPAÑIA
0436	HILDALGO Y ASOCIADOS
4137	INTERNATIONAL AUDITING SERVICES, S.A. DE C.V.
3148	J.PEREZ - AUDITORES Y CONSULTORES ASOCIADOS, S.A. DE C.V.
1987	JOSE REYES MENDEZ Y ASOCIADOS
1391	LINARES VALLE Y COMPAÑIA
1556	LIRA PASASIN Y COMPAÑIA
1703	LOPEZ, QUINTANILLA, ACEVEDO Y COMPAÑIA
2102	LUIS ALONSO REYES RUBIO Y ASOCIADOS
0328	M.A. HIDALGO Y COMPAÑIA
0725	MADRIZ, SALAZAR Y ASOCIADOS CONTADORES PUBLICOS
1217	MARTINEZ, PORTILLO Y ASOCIADOS
0507	MELARA GONZALEZ Y ASOCIADOS
0173	MENA RAMOS Y ASOCIADOS
4217	MENDOZA VASQUEZ, S.A. DE C.V.
4218	MENJIVAR Y MENJIVAR AUDITORES CONSULTORES, S.A. DE C.V.
1218	MERCADILLO MEJIA Y COMPAÑIA
0484	MIRANDA NAVARRO Y COMPAÑIA
1807	MORALES MORENO Y COMPAÑIA
0492	MORALES Y MUÑOZ, ASOCIADOS
2426	MORENO-MORENO-GONZALEZ Y ASOCIADOS
0171	ORELLANA MIXCO Y ASOCIADOS
0341	PAREDES ORELLANA Y ASOCIADOS
3905	PAYMA AUDITORES Y CONSULTORES, S.A. DE C.V.
1806	PERALTA MARROQUIN Y CIA. S.A. DE C.V.
2676	PEREZ HERNANDEZ Y ASOCIADOS
0143	PORTILLO, NOVOA, LOPEZ BERTRAND Y CIA.
0214	PRICEWATERHOUSECOOPERS, S. A. DE C. V.
2498	QUINTANILLA ROQUE Y ASOCIADOS
2398	QUIÑONEZ HENRIQUEZ Y COMPAÑIA
2680	R. MESTIZO Y ASOCIADOS
3397	R.F. SANTOS Y ASOCIADOS
0421	RIVERA MENENDEZ Y COMPAÑIA
1119	RIVERA MUÑOZ Y ASOCIADOS
0748	RIVERA, RAMIREZ, ORTIZ Y ASOCIADOS
1307	RIVERA, LINARES, SIGÜENZA ASOCIADOS
0429	RIVERA, ZACAPA, GONZALEZ Y COMPAÑIA
3195	RODRIGUEZ CELIS ASOCIADOS
0493	ROSALES, VILANOVA, GARCIA Y COMPAÑIA
0477	ROSALES-FLORES Y ASOCIADOS
4195	SALDAÑA & SALDAÑA ASOCIADOS, S.A. DE C.V.
1102	SARAVIA IRAHETA Y ASOCIADOS
2302	SORIANO PERAZA Y COMPAÑIA
3702	TORRES RIVAS Y ASOCIADOS, S.A. DE C.V.
1704	VASQUEZ SALMERON Y ASOCIADOS
2921	VASQUEZ Y ASOCIADOS
2854	VELASQUEZ MURILLO Y COMPAÑIA
1985	VILLALTA RODRIGUEZ Y ASOCIADOS

ANEXO 2

Encuesta de investigación

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE CONTADURÍA PÚBLICA

CUESTIONARIO

DIRIGIDO A: Las firmas de auditoría con personería jurídica autorizadas por el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría.

OBJETIVO: Obtener información relevante de como las firmas de auditoría con personería jurídica aplican la NIA 315, en lo relativo a la identificación y evaluación de riegos de tecnologías de información (TI), cuando ejecuten encargos a empresas que posean sistemas automatizados relevantes a la información financiera que presentan.

PROPÓSITO: La presente guía de preguntas ha sido elaborada por estudiantes de la carrera de licenciatura de contaduría pública, con el propósito de sustentar el trabajo de investigación relativo a la identificación y evaluación de riesgos de tecnologías de información relevantes en una auditoría de estados financieros.

INDICACIONES: Marque con una "X" la(s) respuesta(s) que usted considere más conveniente o complementar según el caso.

1. ¿Realizan auditorías a empresas en las cuales la información financiera depende en algún grado del uso de tecnologías de información (TI) o sistemas contables computarizados?

   SI ☐ NO ☐

2. ¿En qué medida se considera el uso de TI en la información financiera de sus clientes al momento de la planeación de auditoría?

   a) Bastante ☐ c) Poco ☐

   b) Regular ☐ d) Nada ☐

3. Si de alguna medida considera la TI conforme a la pregunta anterior, ¿bajo qué enfoque basan la consideración de aspectos relativos a tecnologías de información? Puede seleccionar más de una opción.

   a) COBIT (Objetivos de control para tecnología y áreas relacionadas) ☐
   b) ITIL (Gestión de servicios de TI) ☐
   c) ISO 27001/27002 (Sistema de gestión para la seguridad de la información) ☐
   d) COSO ☐
   e) COSO ERM ☐
   f) Otros ☐

   Especifique _____

4. Como parte del proceso de evaluación del control interno, ¿incluyen el área relacionada a tecnologías de información?

   SI ☐ NO ☐

5. Si su respuesta a la pregunta anterior fue negativa, ¿cuáles han sido los motivos por los que no ha considerado el aspecto informático en la evaluación del control interno? Puede seleccionar más de una opción.

   a) Falta de personal capacitado ☐
   b) Falta de herramientas tecnológicas ☐
   c) Otros ☐

   Especifique: _____

6. Si su respuesta a la pregunta 4 es afirmativa, ¿qué componentes del control interno informático son considerados? Puede seleccionar más de una opción.

   a) Análisis, desarrollo e implementación de sistemas ☐
   b) Evaluación de los controles sobre las operaciones que se realizan en los sistemas ☐
   c) Procedimientos de entrada de datos ☐
   d) Procesamiento de la información ☐

e) Emisión de resultados (reportes) ☐

f) Seguridad del área de sistemas ☐

g) Otros ☐

Especifique: _____

7. En relación a la pregunta número 6, ¿se hace necesario el uso de un experto para este tipo de evaluaciones del control interno?

SI ☐ NO ☐

8. ¿Hace uso de las técnicas de auditoría asistidas por computador (TAAC´s) en la planeación de una auditoría de estados financieros?

SI ☐ NO ☐

9. ¿Utilizan software especializado en analizar pistas de auditoría para desarrollar sus trabajos?

SI ☐ NO ☐

10. Si su respuesta a la pregunta 9 es afirmativa, ¿cuáles utilizan? Puede seleccionar más de una opción.

a) IDEA ☐

b) ACL ☐

c) Otros ☐

Especifique: _____

11. De la siguiente lista, ¿en cuáles áreas ha recibido o recibe educación continuada? Puede seleccionar más de una opción.

a)	Informática	☐	f)	Auditoría Interna	☐
b)	Contabilidad	☐	g)	Auditoría Forense	☐
c)	Finanzas	☐	h)	Administración de Riesgos	☐
d)	Auditoría Externa	☐	i)	Impuestos	☐

12. Como profesionales en contaduría pública, al momento de ejecutar auditoría de estados financieros, ¿ha considerado los aspectos que establece la Declaración sobre las Prácticas Internacionales de Formación No. 2 (IEPS2) titulada "Tecnología de la Información para Contadores Profesionales" emitida por IFAC?

    SI ☐ NO ☐

13. Si su respuesta a la pregunta 12 es negativa, ¿cuáles son las razones de no considerar los aspectos establecidos en la Declaración sobre las Prácticas Internacionales de Formación No. 2 (IEPS2)? Puede seleccionar más de una opción.

    a) Insuficiente material de apoyo ☐
    b) Desconocimiento de la normativa ☐
    c) Falta de herramientas para aplicarla ☐

14. ¿Cuáles son las dificultades que existen, al momento de evaluar el control interno de sus clientes respecto al área de tecnología de información y comunicación? Puede seleccionar más de una opción.

    a) Riesgo de Fraude ☐
    b) Aseveraciones ☐
    c) Falta o mala aplicación de políticas contables ☐
    d) Integridad de la información ☐

15. Si su respuesta a la pregunta 12 es afirmativa, ¿cuáles son las principales dificultades que considera pertinentes? Puede seleccionar más de una opción.

    a) Ausencia de educación continuada ☐
    b) Educación superior desactualizada ☐
    c) Falta de bibliografía técnica aplicable ☐
    d) Otros ☐

    Especifique: _____

16. ¿Ordene por grado de importancia en escala del 1 al 5 los factores que considere indispensables para realizar una evaluación de riesgos en el área de tecnología de información durante la ejecución de una auditoría de estados financieros?

    a) Exigencia de la normativa técnica ☐
    b) Indicios de fraude en el área de TI ☐
    c) Creciente dependencia del negocio con respecto a las tecnologías de información ☐
    d) Carencia de controles del negocio con respecto a las tecnologías de información ☐
    e) Dificultades presentes en el personal de TI ☐

17. ¿Considera que existe material adecuado o información bibliográfica suficiente, para auxiliarse en la correcta identificación y evaluación de riesgo informáticos?

    SI ☐ NO ☐

18. ¿Considera necesario y útil para la firma contar con una metodología de orientación para la identificación y evaluación de riesgos de tecnologías de información, cuando se realicen auditorías a la información financiera bajo un ambiente de sistemas computarizados?

    SI ☐ NO ☐

19. Para el establecimiento de la materialidad de auditoría, ¿considera o toma en cuenta los riesgos relacionados al área de tecnología de información?

    SI ☐ NO ☐

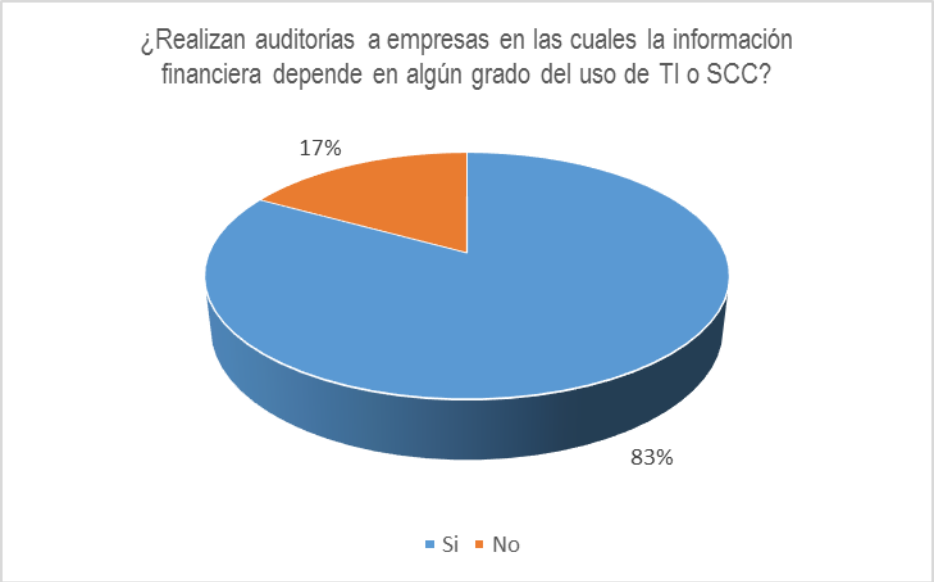
ANEXO 3

Análisis e interpretación de datos

Pregunta No. 1 ¿Realizan auditorías a empresas en las cuales la información financiera depende en algún grado del uso de tecnologías de información (TI) o sistemas contables computarizados?

Objetivo: Conocer el porcentaje de firmas que realizan auditorías a entidades que poseen la información financiera en un ambiente de TI o sistemas contables computarizados.

Categoría	Frecuencia absoluta	Frecuencia relativa
Si	49	83%
No	10	17%
Total	**59**	**100%**

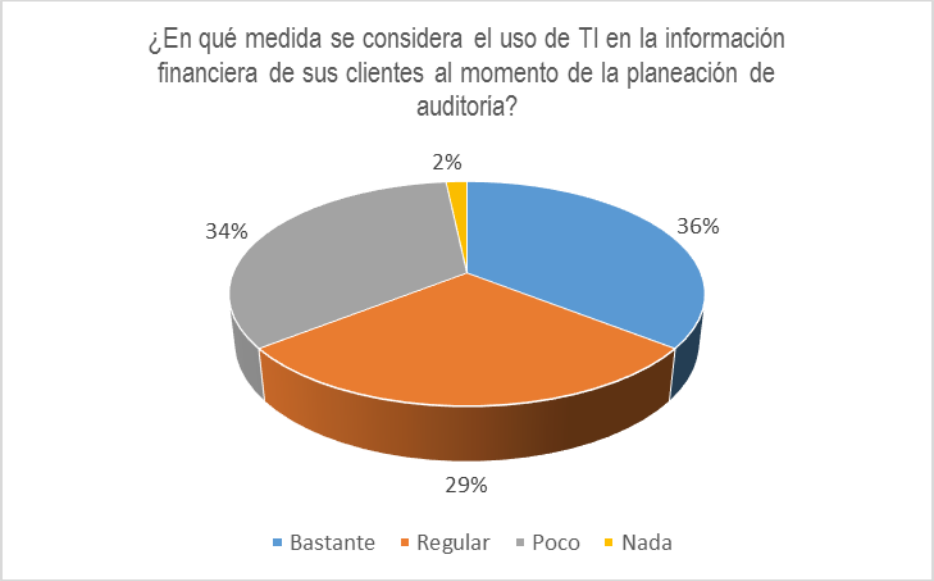


Interpretación: Más del ochenta por cierto de las firmas trabajan con información financiera procesada en alguna medida a través del uso de TI, por parte de sus clientes, lo cual confirma la creciente dependencia de las tecnologías de información y comunicación en los negocios.

Pregunta No. 2 ¿En qué medida se considera el uso de TI en la información financiera de sus clientes al momento de la planeación de auditoría?

Objetivo: Indagar el nivel con el que las firmas consideran los aspectos tecnológicos al momento de planificar una auditoría.

Categoría	Frecuencia absoluta	Frecuencia relativa
Bastante	21	36%
Regular	17	29%
Poco	20	34%
Nada	1	2%
Total	**59**	**100%**

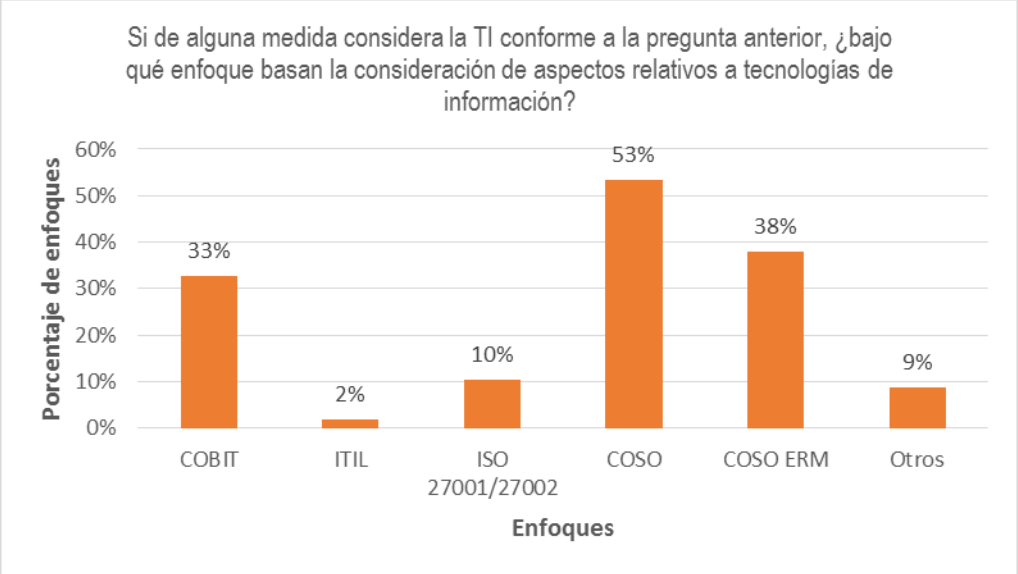


Interpretación: Al momento de elaborar la planeación, las firmas ejercen un nivel limitado sobre aspectos tecnológicos utilizados para la información financiera de sus clientes, el 36% considera bastante el uso de TI, mientras que el 34% considera que aplica poco la consideración de TI en sus estrategias de planeación.

Pregunta No. 3. Si de alguna medida considera la TI conforme a la pregunta anterior, ¿bajo qué enfoque basan la consideración de aspectos relativos a tecnologías de información? Puede seleccionar más de una opción.

Objetivo: Conocer el enfoque bajo el cual las firmas basan la consideración de aspectos relativos a tecnologías de información en la ejecución de encargos de auditoría de estados financieros.

Categoría	Resultado	Porcentaje
COBIT	19/58	33%
ITIL	1/58	2%
ISO 27001/27002	6/58	10%
COSO	31/58	53%
COSO ERM	22/58	38%
Otros	5/58	9%

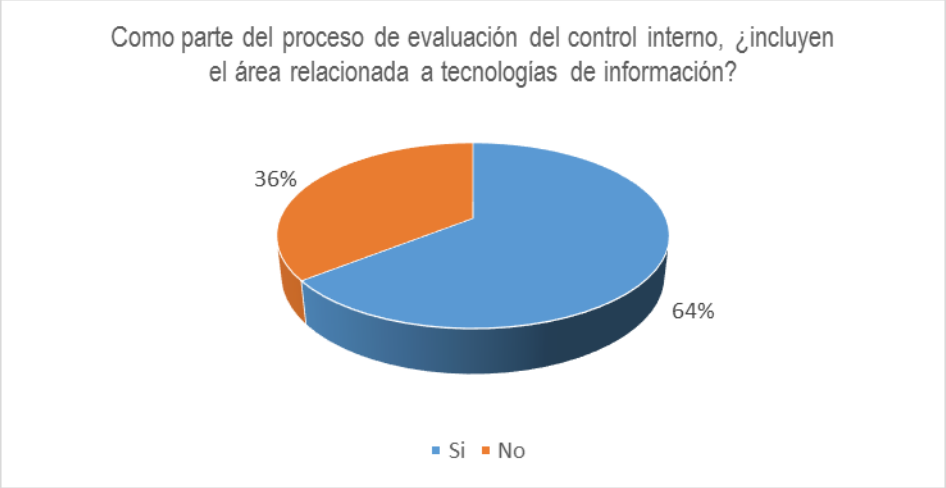


Interpretación: Para aquellas firmas que contemplan la TI en su planeación como bastante (36%) y regular 29%, se enfocan principalmente en los marcos de referencia COSO-ERM y COBIT respectivamente, otras firmas consideran en menor grado ITIL e ISO. La NIA 315 permite hacer uso de cualquier forma de evaluación de riesgos, respetando los principios: a) ambiente de control; b) el proceso de evaluación del riesgo por la entidad; c) el sistema de información; d) actividades de control; e) monitoreo de controles.

Pregunta No. 4. Como parte del proceso de evaluación del control interno, ¿incluyen el área relacionada a tecnologías de información?

Objetivo: Conocer si en la actualidad las firmas de auditoría consideran al aspecto informático en la evaluación del control interno de las entidades que auditan.

Categoría	Frecuencia absoluta	Frecuencia relativa
Si	38	64%
No	21	36%
Total	**59**	**100%**

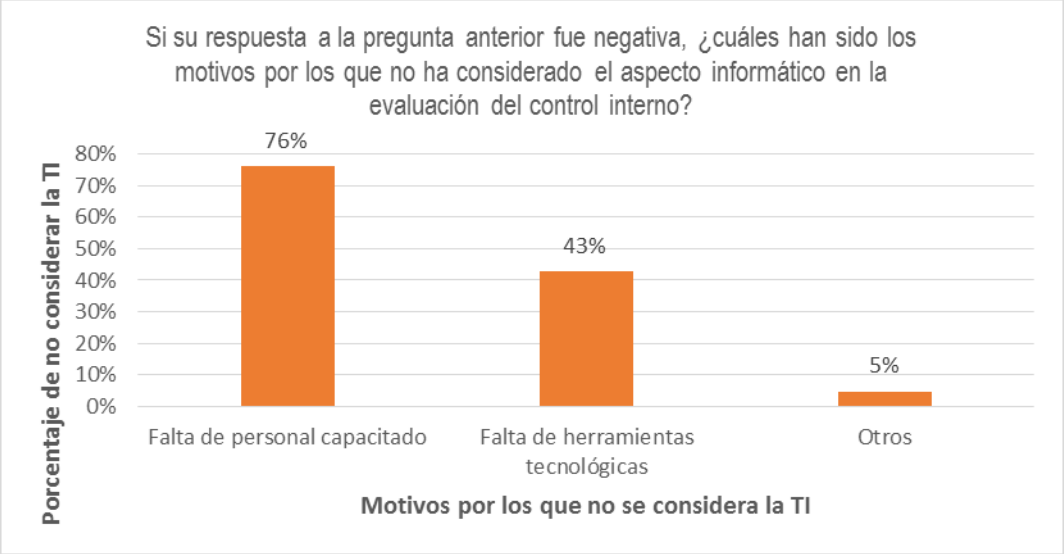


Interpretación: Actualmente poco más de la mitad de las firmas realiza evaluaciones del control interno de tecnología de información relevante utilizado por sus clientes. Sin embargo, el análisis que se considera el ambiente de TI como parte del conocimiento del negocio en la planeación, no indica que las firmas incluyen el resultado de la evaluación del control interno, es decir la detección e identificación de riesgos.

Pregunta No. 5. Si su respuesta a la pregunta anterior fue negativa, ¿cuáles han sido los motivos por los que no ha considerado el aspecto informático en la evaluación del control interno? Puede seleccionar más de una opción.

Objetivo: Indagar sobre los motivos por los que las firmas no consideran el aspecto informático en la evaluación del control interno.

Categoría	Resultado	Porcentaje
Falta de personal capacitado	16/21	76%
Falta de herramientas tecnológicas	9/21	43%
Otros	1/21	5%

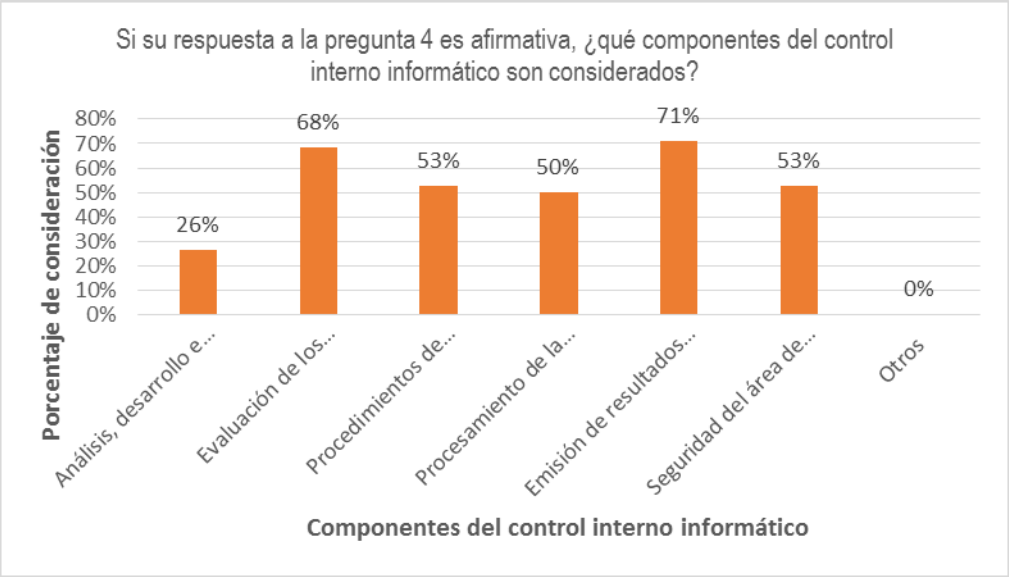


Interpretación: Los motivos por el que las firmas no evalúan el control interno TI, se debe primordialmente al insuficiente personal capacitado que poseen, y en segundo orden, a que no tienen las suficientes herramientas tecnológicas, motivo por el cuál las firmas indicaron en la pregunta número dos seleccionando la opción "bastante" sólo en un 36% de las ocasiones, cuando se les indagaba si aplicaban la consideración de riesgos de TI en la planeación de auditoría.

Pregunta No. 6. Si su respuesta a la pregunta 4 es afirmativa, ¿qué componentes del control interno informático son considerados? Puede seleccionar más de una opción.

Objetivo: Identificar las áreas que son consideradas en la evaluación del control interno informático.

Categoría	Resultado	Porcentaje
Análisis, desarrollo e implementación de sistemas	10/38	26%
Evaluación de los controles sobre las operaciones que realizan en los sistemas	26/38	68%
Procedimientos de entrada de datos	20/38	53%
Procesamiento de la información	19/38	50%
Emisión de resultados (reportes)	27/38	71%
Seguridad del área de sistemas	20/38	53%
Otros	0/38	0%

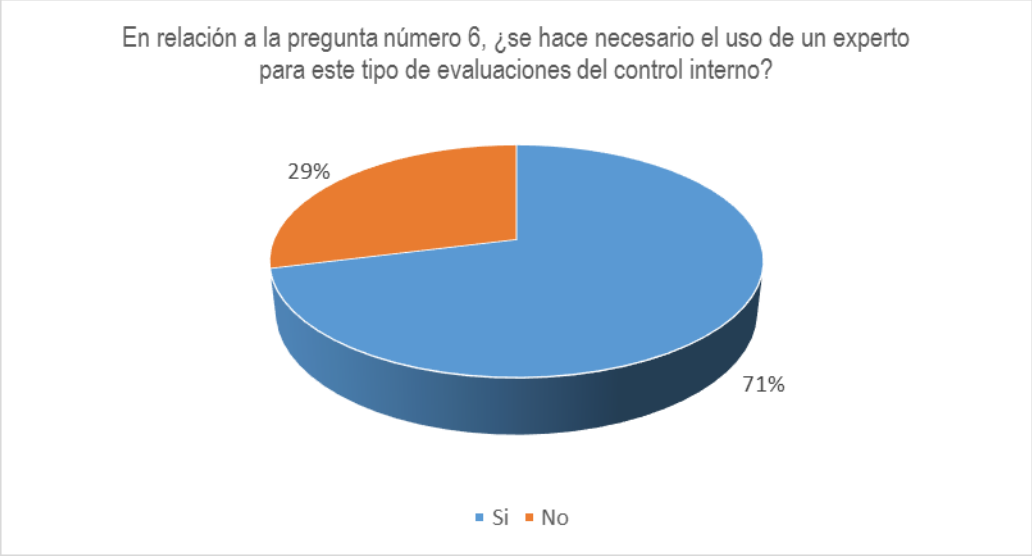


Interpretación: Las firmas que si evalúan el control interno TI de sus clientes 38/59, centralizan sus esfuerzos en el área de reportes que genera el sistema información, seguido de la evaluación del control interno relevante y los procedimientos de entrada de información.

Pregunta No. 7. En relación a la pregunta número 6, ¿se hace necesario el uso de un experto para este tipo de evaluaciones del control interno?

Objetivo: Conocer el tipo de personal que realiza la evaluación del control interno informático.

Categoría	Frecuencia absoluta	Frecuencia relativa
Si	27	71%
No	11	29%
Total	**38**	**100%**

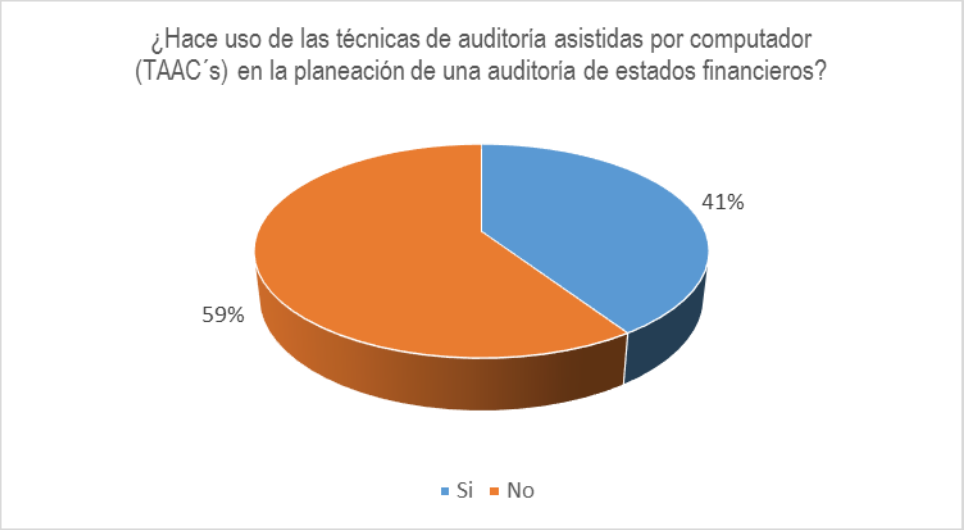


Interpretación: Estos esfuerzos por evaluar el control interno TI de sus clientes, es posible gracias al apoyo del experto del auditor, una pequeña parte de estas firmas evalúa por cuenta propia dichos controles, sin embargo esto no inhibe al encargado de auditoría de conocer sobre evaluación de riesgos de TI, debido a que según la normativa es el encargado el responsable de la estrategia de auditoría que incluye la consideración de riesgos. Es por tal motivo que las personas encuestadas según la pregunta número 2, las firmas indicaron que consideraron en un 34% que aplican "poco" la consideración de riesgos de TI en la planeación.

Pregunta No. 8 ¿Hace uso de las técnicas de auditoría asistidas por computador (TAAC´s) en la planeación de una auditoría de estados financieros?

Objetivo: Indagar sobre el uso de las TAAC´s en la fase de planeación de una auditoría de estados financieros.

Categoría	Frecuencia absoluta	Frecuencia relativa
Si	24	41%
No	35	59%
Total	**59**	**100%**



Interpretación: Del 64% de las firmas que consideran al aspecto informático en sus auditorías (ver pregunta 4) únicamente el 41% hacen uso de técnicas de auditoría asistidas por computador para la planeación de los encargos.

Pregunta No. 9 ¿Utilizan software especializado en analizar pistas de auditoría para desarrollar sus trabajos?

Objetivo: Conocer sobre el uso de algún sistema especializado para desarrollar todo un trabajo de auditoría.

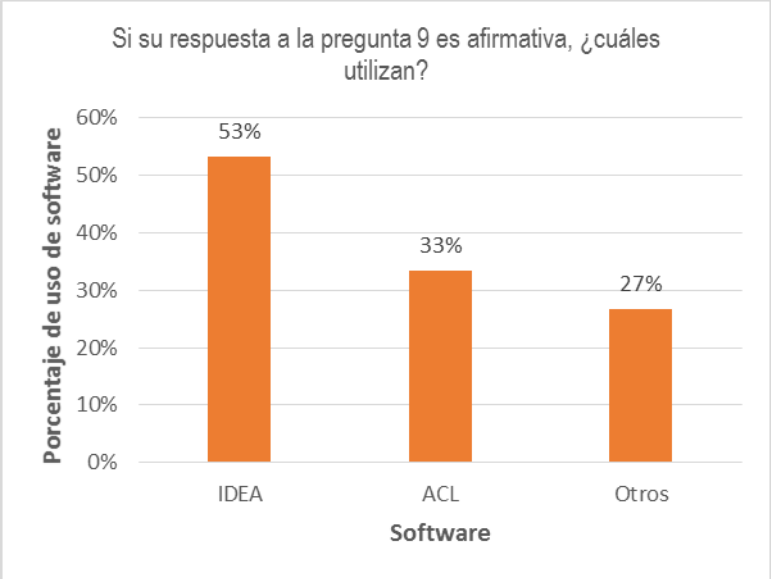
Categoría	Frecuencia absoluta	Frecuencia relativa
Si	15	25%
No	44	75%
Total	**59**	**100%**

Interpretación: Del 41% de firmas que hacen uso de TAAC´s (ver pregunta 8) al menos una cuarta parte de ellas manifiestan haber utilizado software especializado para el análisis de pistas de auditoría. Esto es congruente con el hecho de que el 65% de las firmas consideran poco, regular o nulo uso de la TI en la planeación de auditoría (ver pregunta 2).

Pregunta No. 10. Si su respuesta a la pregunta 9 es afirmativa, ¿cuáles utilizan? Puede seleccionar más de una opción.

Objetivo: Conocer el o los software especializados más utilizados para desarrollar trabajos de auditoría.

Categoría	Resultado	Porcentaje
IDEA	8/15	53%
ACL	5/15	33%
Otros	4/15	27%

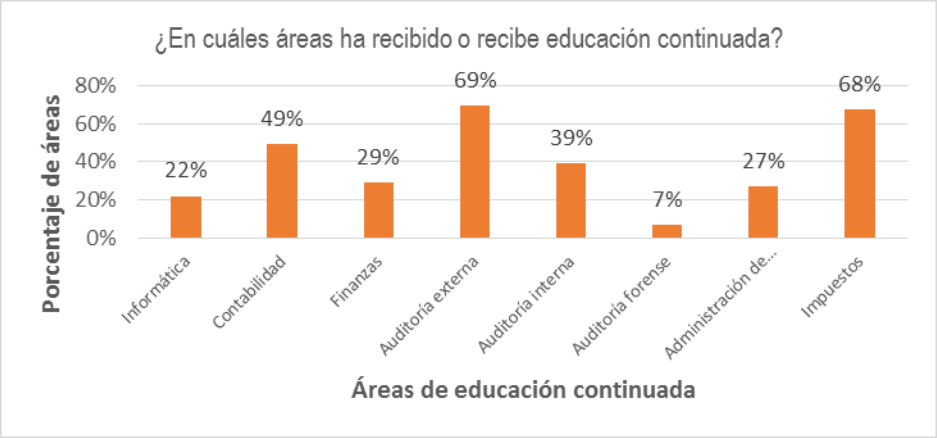


Interpretación: El 25% de las firmas que manifiestan usar software especializado en analizar pistas de auditoría (ver pregunta 9) declaran que, en su mayoría, utilizan el programa computacional IDEA, el resto hace uso del sistema ACL u otro adicional (entre ellos AS/2 Audit sistems, winaudit, netscan, came). Este resultado concuerda con el limitado nivel de consideración de los aspectos tecnológicos que las firmas hacen en sus auditorías (ver pregunta 2).

Pregunta No. 11. De la siguiente lista, ¿en cuáles áreas ha recibido o recibe educación continuada? Puede seleccionar más de una opción.

Objetivo: Conocer las principales áreas donde los profesionales autorizados, obtienen conocimiento mediante la educación continuada y específicamente saber si se capacitan en áreas de tecnología de información.

Categoría	Resultado	Porcentaje
Informática	13/59	22%
Contabilidad	29/59	49%
Finanzas	17/59	29%
Auditoría externa	41/59	69%
Auditoría interna	23/59	39%
Auditoría forense	4/59	7%
Administración de riesgos	16/59	27%
Impuestos	40/59	68%



Interpretación: Las principales áreas de educación continuada entre los profesionales de auditoría son los impuestos y la auditoría de estados financieros, una de las áreas más descuidadas es la informática, ya que solo el 22% recibe capacitación constante en esa materia. Debido a ello, 7 de cada 10 firmas manifiestan que la falta de personal capacitado en informática es el principal motivo por el que no consideran el aspecto TI en sus clientes (ver pregunta 5), para solventar este desfase, el 71% de los tales hace uso de un experto para las evaluaciones de control interno de este tipo (ver pregunta 7).

Pregunta No. 12. Como profesionales en contaduría pública, al momento de ejecutar auditoría de estados financieros, ¿ha considerado los aspectos que establece la Declaración sobre las Prácticas Internacionales de Formación No. 2 (IEPS2) titulada "Tecnología de la Información para Contadores Profesionales" emitida por IFAC?

Objetivo: Conocer si las firmas con personería jurídica en la actualidad al momento de ejecutar un trabajo de auditoría consideran los aspectos que establece la IEPS 2.

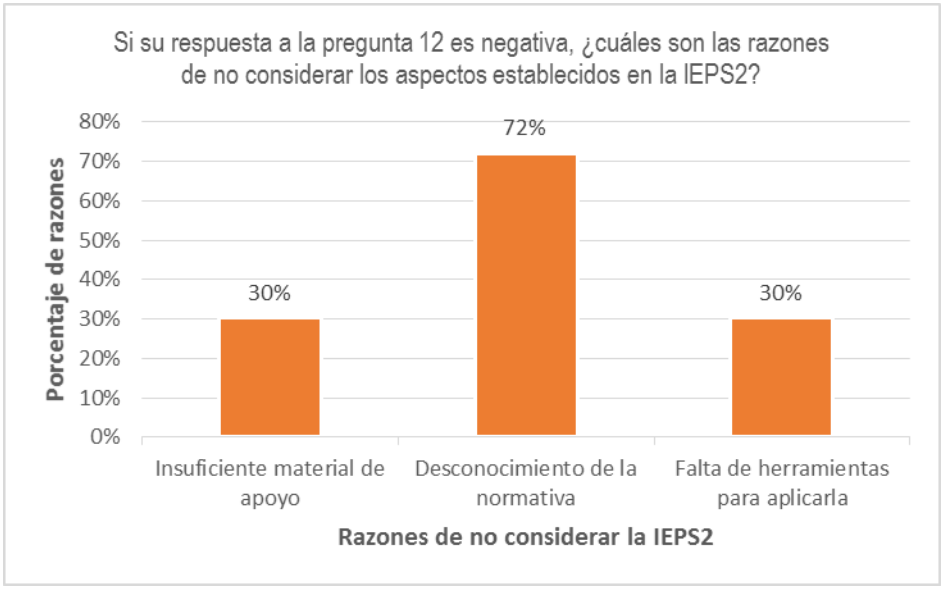
Categoría	Frecuencia absoluta	Frecuencia relativa
Si	16	27%
No	43	73%
Total	**59**	**100%**

Interpretación: A raíz de que solo 2 de cada 10 firmas poseen capacitación constante en el área informática (Ver pregunta 11), trae como consecuencia que solo el 27% pueda considerar los aspectos que establece la IEPS 2.

Pregunta No. 13. Si su respuesta a la pregunta 12 es negativa, ¿cuáles son las razones de no considerar los aspectos establecidos en la Declaración sobre las Prácticas Internacionales de Formación No. 2 (IEPS2)? Puede seleccionar más de una opción.

Objetivo: Conocer los principales motivos presentados a los profesionales para la aplicación de la IEPS2 relacionado con la tecnología de información y en consecuencia, conocer el grado de aplicación sobre la misma.

Categoría	Resultado	Porcentaje
Insuficiente material de apoyo	13/43	30%
Desconocimiento de la normativa	31/43	72%
Falta de herramientas para aplicarla	13/43	30%

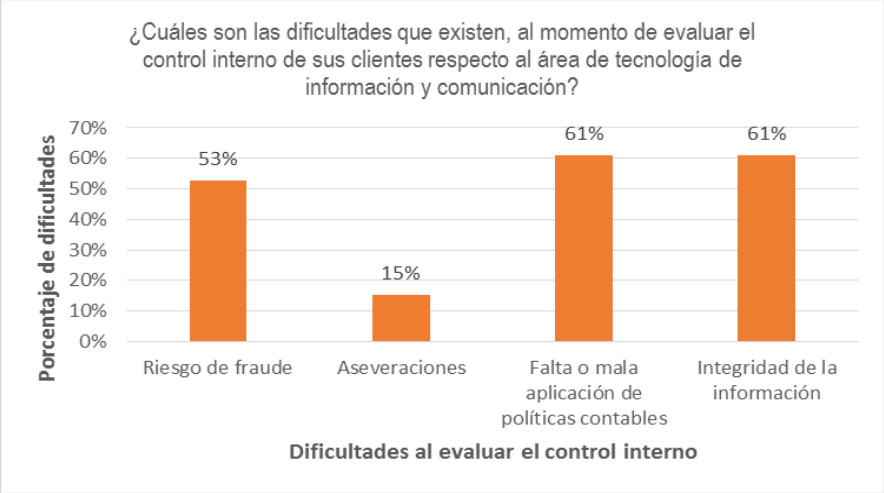


Interpretación: debido a que únicamente el 22% de las firmas mantienen educación continuada en el área informática (ver pregunta 11), hace que el 72% de ellas desconozcan completamente la normativa, considerándose como la razón principal del porque no puedan aplicar la IEPS 2. En menor medida, el insuficiente material de apoyo y la falta de herramientas, constituyen elementos importantes de la no aplicación.

Pregunta No. 14 ¿Cuáles son las dificultades que existen, al momento de evaluar el control interno de sus clientes respecto al área de tecnología de información y comunicación? Puede seleccionar más de una opción.

Objetivo: Indagar sobre la existencia de dificultades en la evaluación del riesgo en componentes relacionados con la TI.

Categoría	Resultado	Porcentaje
Riesgo de fraude	31/59	53%
Aseveraciones	9/59	15%
Falta o mala aplicación de políticas contables	36/59	61%
Integridad de la información	36/59	61%

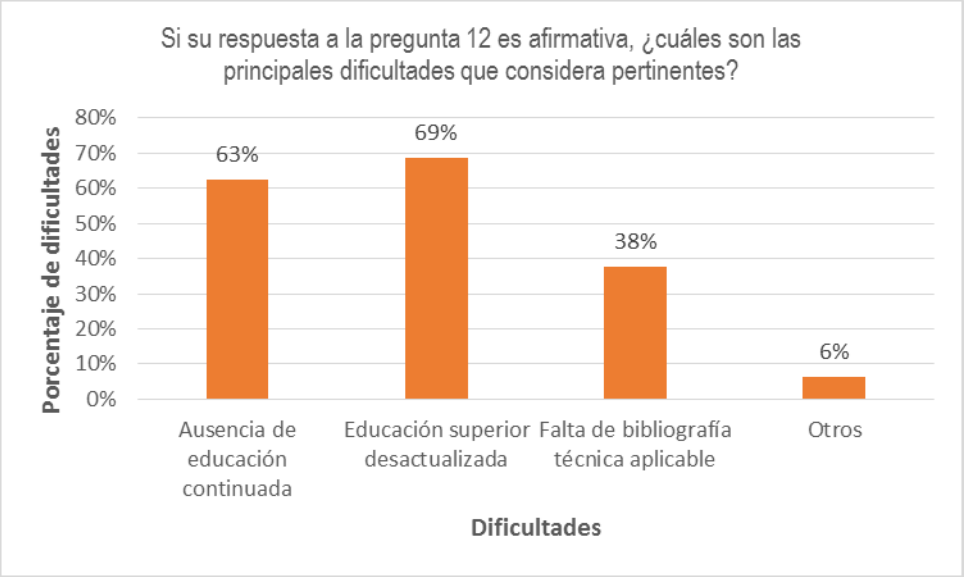


Interpretación: Como parte del proceso de evaluación del control interno que las firmas de auditoría realizan a las TIC´s relevante a la información financiera de sus clientes, los auditores consideran que las principales dificultades existentes son la falta o mala aplicación de las políticas contables y la integridad de la información en igual importancia, seguidos de los riesgos de fraude; esto es como consecuencia de que en la actualidad los usuarios se adaptan a los sistemas y no lo contrario. Sim embargo, cabe destacar que solamente el 15% de dichas firmas piensan que las aseveraciones hechas por la administración de sus clientes representan mayores dificultades en dicha evaluación

Pregunta No. 15. Si su respuesta a la pregunta 12 es afirmativa, ¿cuáles son las principales dificultades que considera pertinentes? Puede seleccionar más de una opción.

Objetivo: Conocer sobre las principales dificultades por las que no se evalúan los riesgos de TI.

Categoría	Resultado	Porcentaje
Ausencia de educación continuada	10/16	63%
Educación superior desactualizada	11/16	69%
Falta de bibliografía técnica aplicable	6/16	38%
Otros	1/16	6%

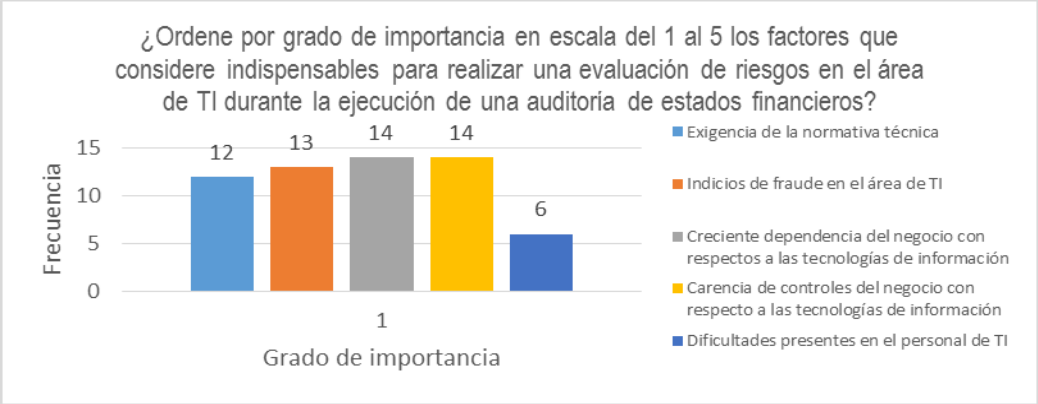


Interpretación: Las firmas se enfrentan a dificultades al momento de aplicar la IEPS2, entre los que cabe destacar la educación superior desactualizada y la usencia de educación continuada, ya que como se muestra en los resultados de la pregunta No. 1 se realizan auditorías en un 83% a empresas que de alguna manera tienen automatizada la información financiera, por lo consiguiente el personal de auditoría necesita tener mayor competencia para evaluar los aspectos relacionados con la TI.

Pregunta No. 16 ¿Ordene por grado de importancia en escala del 1 al 5 los factores que considere indispensables para realizar una evaluación de riesgos en el área de tecnología de información durante la ejecución de una auditoría de estados financieros?

Objetivo: Conocer el grado de consideración que las firmas le dan a los factores que intervienen en la evaluación de riesgos de TI.

Categoría	1	2	3	4	5
Exigencia de la normativa técnica	12	5	18	9	15
Indicios de fraude en el área de TI	13	11	10	16	9
Creciente dependencia del negocio con respectos a las tecnologías de información	14	15	8	8	14
Carencia de controles del negocio con respecto a las tecnologías de información	14	16	10	12	7
Dificultades presentes en el personal de TI	6	12	13	14	14

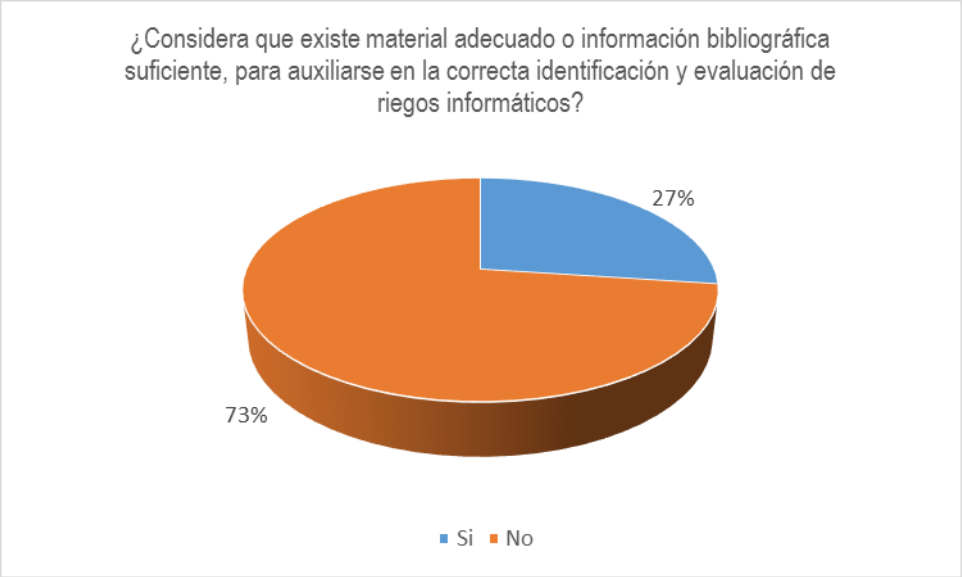


Interpretación: Aclarando que la opción 1 es más importante y la 5 de menor importancia, no existe ninguna diferencia en cuanto a determinar cuál es el grado de importancia pues todas las categorías se muestran prácticamente con la misma fuerza; excepto en las dificultades presentes en el personal de TI debido a que las firmas hacen uso de un experto como lo manifiestan los resultados de la pregunta No. 7. También llama la atención que el indicio de fraude en el área de tecnología es bien importante y esto se ve reflejado con los resultados de la pregunta No. 14 en la cual el 53% afirma que es un área de alto riesgo.

Pregunta No. 17 ¿Considera que existe material adecuado o información bibliográfica suficiente, para auxiliarse en la correcta identificación y evaluación de riesgo informáticos?

Objetivo: Indagar sobre la suficiencia del material para la identificación y evaluación de riesgos de TI.

Categoría	Frecuencia absoluta	Frecuencia relativa
Si	16	27%
No	43	73%
Total	**59**	**100%**

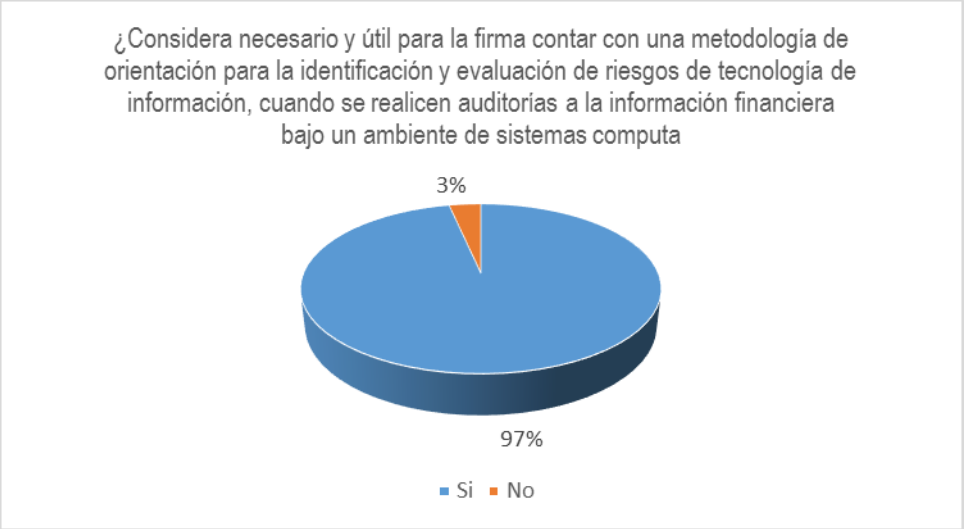


Interpretación: El 73% de las firmas de auditoría con personería jurídica consideran que en la actualidad no existe el material adecuado y suficiente para auxiliarse en la correcta identificación y evaluación de riesgos de tecnología de información.

Pregunta No. 18 ¿Considera necesario y útil para la firma contar con una metodología de orientación para la identificación y evaluación de riesgos de tecnologías de información, cuando se realicen auditorías a la información financiera bajo un ambiente de sistemas computarizados?

Objetivo: Identificar la necesidad de contar con una metodología en cumplimiento con Normas Internacionales de Auditoría y basada en COBIT 5 para identificar y evaluar riesgos de TI cuando la información financiera se encuentra en un ambiente computarizado.

Categoría	Frecuencia absoluta	Frecuencia relativa
Si	57	97%
No	2	3%
Total	**59**	**100%**

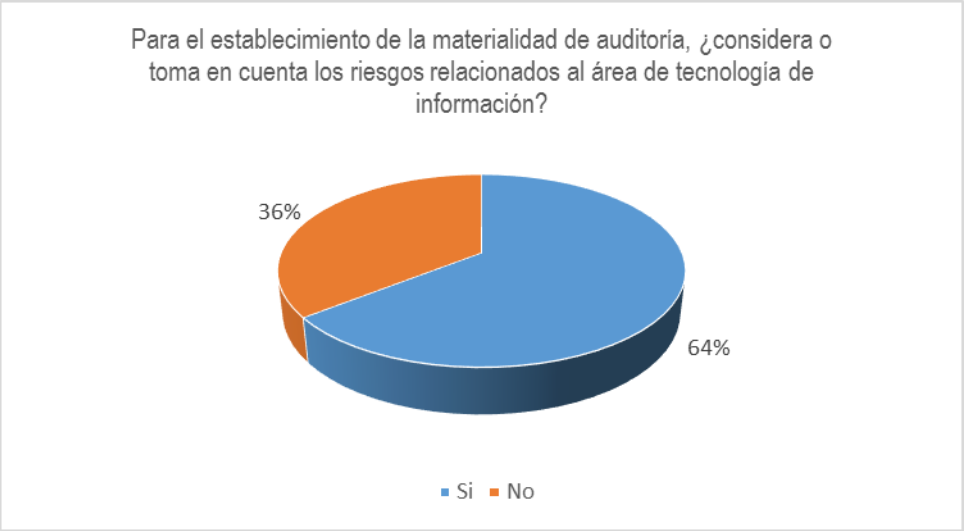


Interpretación: Aunque el 27% de las firmas según pregunta No. 17 de nuestra investigación manifiestan que existe el material adecuado y suficiente para la identificación y evaluación de riesgos de TI, el 97% considera necesaria y útil una metodología que les oriente en la ejecución de auditorías a la información financiera bajo un ambiente de sistemas computarizados, ya que al considerar dicha evaluación se han visto en la necesidad de que el no contar con un instrumento básico les dificulta realizar su trabajo aplicado a normativa.

Pregunta No. 19. Para el establecimiento de la materialidad de auditoría, ¿considera o toma en cuenta los riesgos relacionados al área de tecnología de información?

Objetivo: Indagar acerca de la consideración de los riesgos de tecnología de información en el establecimiento de la materialidad.

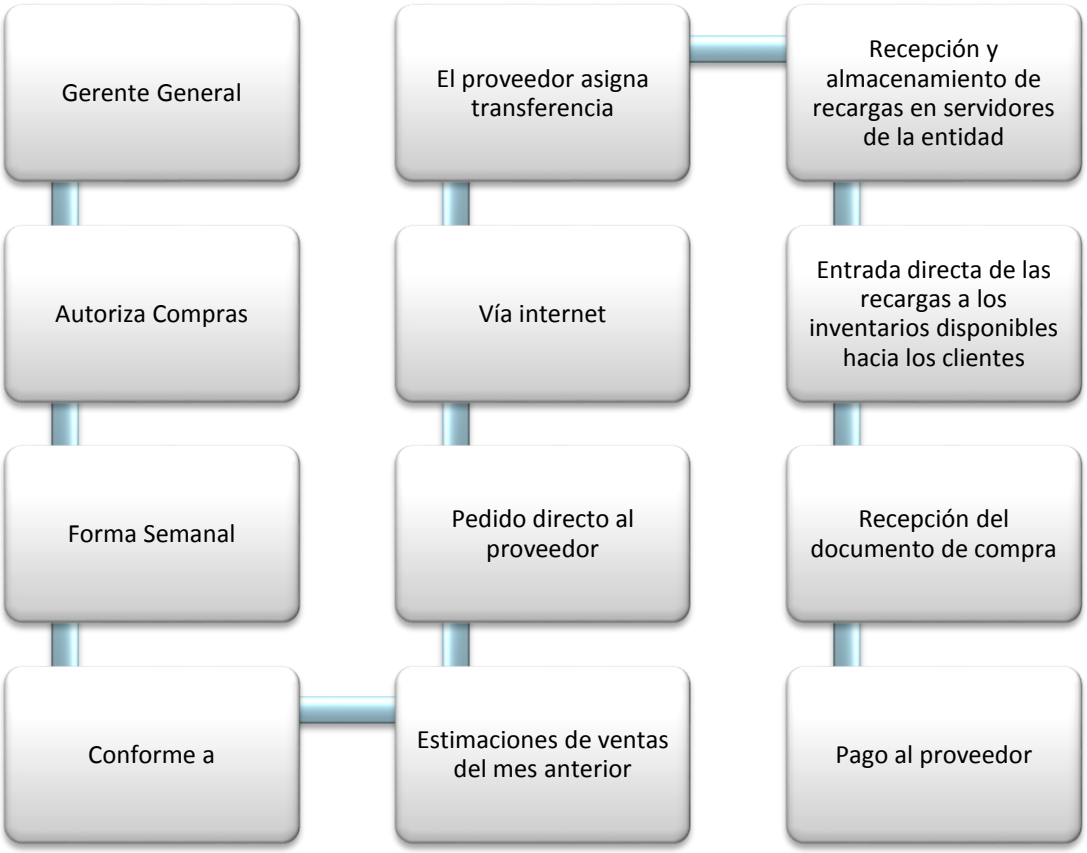
Categoría	Frecuencia absoluta	Frecuencia relativa
Si	38	64%
No	21	36%
Total	**59**	**100%**



Interpretación: Según se muestra en el gráfico 6 de cada 10 firmas de auditoría consideran en la materialidad los riesgos relacionados con la TI, lo cual es congruente con los resultados de la pregunta No.2 ya que un 36% consideran los aspectos tecnológicos en la planeación de la auditoría, pero con base en la pregunta No. 7 se ven en la necesidad de auxiliarse de un experto.

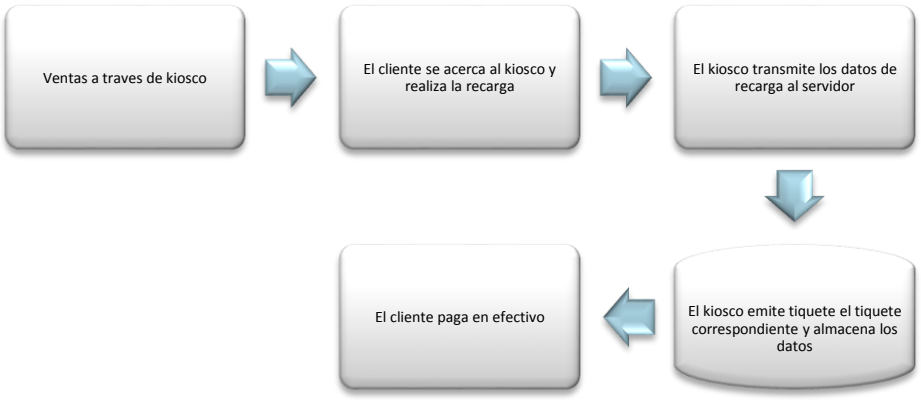
ANEXO 4

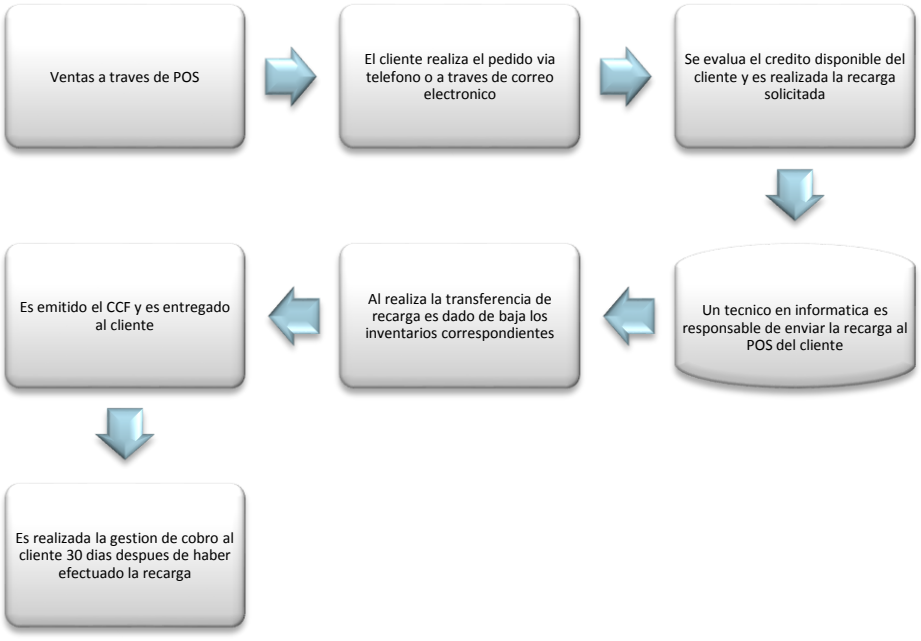
Proceso de compras de Recarga Directa, S.A. de C.V.



ANEXO 5

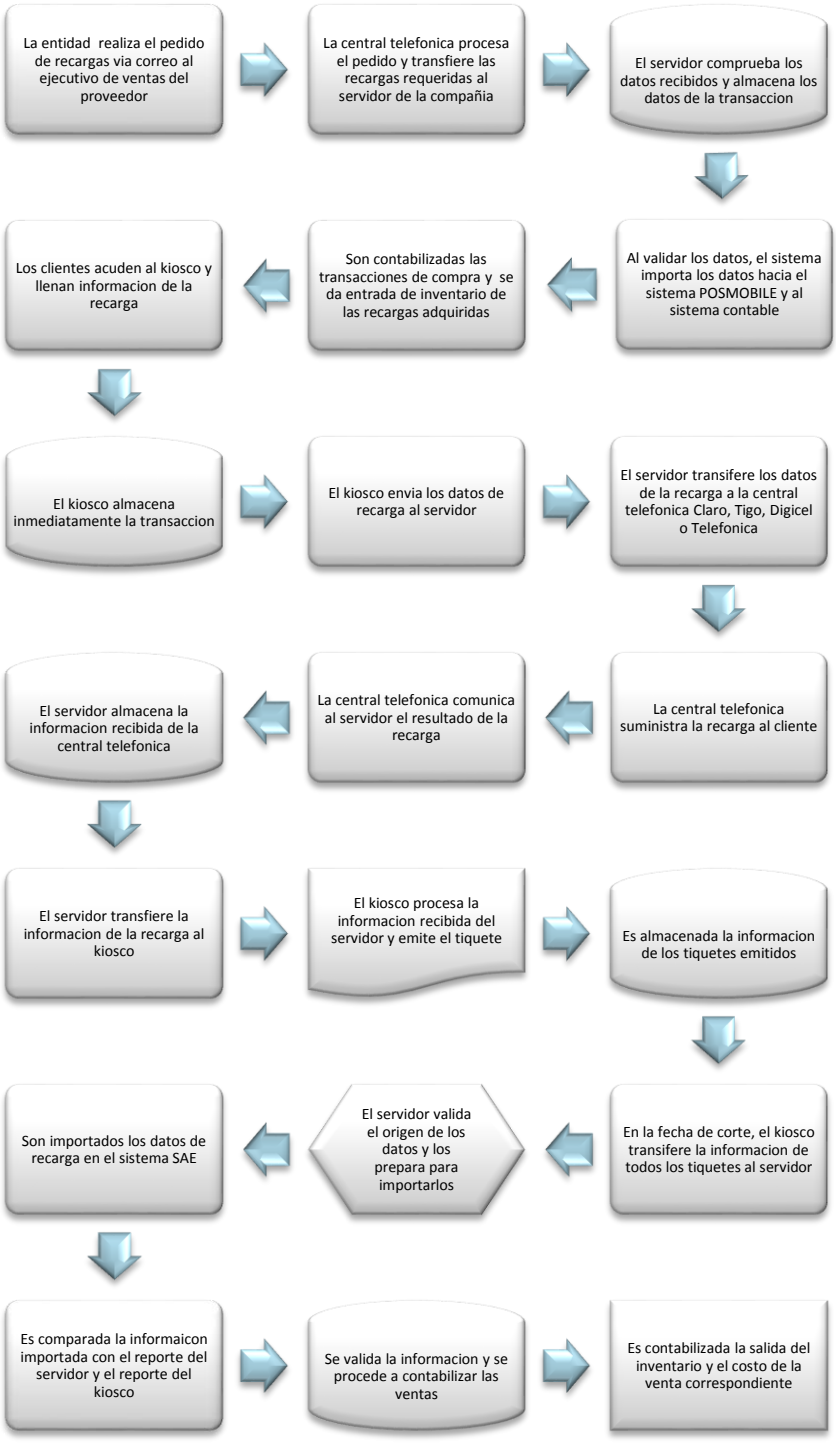
Proceso de ventas de Recarga Directa, S.A. de C.V.





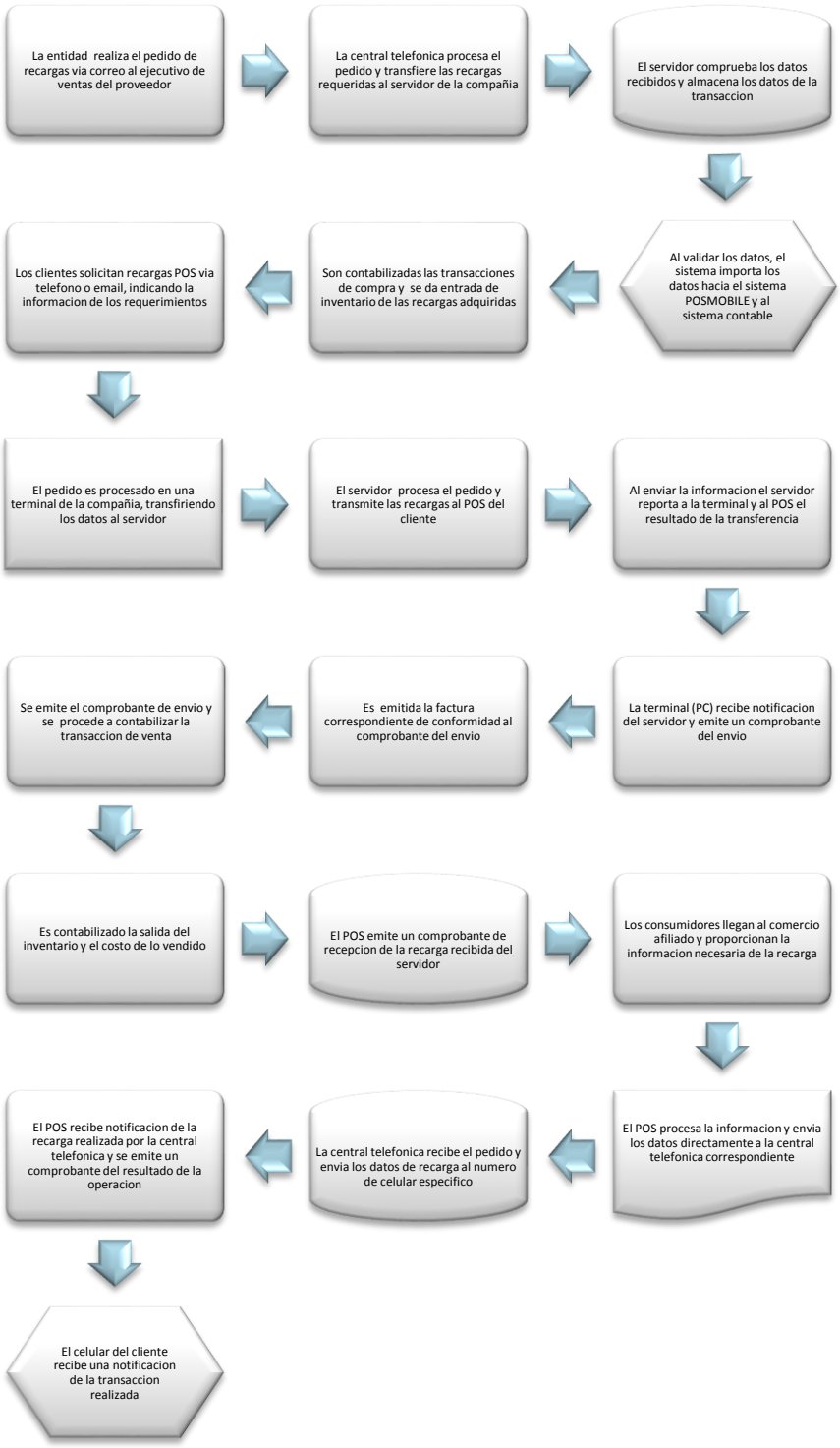
ANEXO 6

Ciclo de la información para las recargas de POS.



ANEXO 7

Ciclo de la información para las recargas en kioskos



ANEXO 8

Procedimientos analíticos para obtención de conocimiento de la entidad.

ANEXO 8.1

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

PROGRAMA DE SEGURIDAD DEL SISTEMA

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0	2012	PSS

OBJETIVO: Determinar el nivel de seguridad a nivel de privilegios de usuario que la entidad ha establecido en sus sistemas informáticos.

ALCANCE: Serán analizados todos los usuarios registrados en el sistema.

N°	Procedimiento	Ref. Cuest.	Ref.	Hecho por
1	Solicite acceso a la tabla de perfiles de usuario del sistema.		PS1	LJG
2	Revise en los perfiles de usuario quienes son los autorizados para acceder a los campos de parametrización.		PS2	LJG
3	Revise en los perfiles de usuario si los privilegios establecidos están de acuerdo a los roles y responsabilidades del usuario.		PS3	LJG
4	Verifique cuantos administradores o super usuarios del sistema existen.		PS4	LJG
5	Indague acerca de la política empresarial para establecer nombres de usuario, por ejemplo: nombre y apellido, primer letra del apellido y nombre completo, etc.		PS5	LJG
6	Verifique si los nombres de usuarios cumplen con la política de la empresa previamente establecida.		PS6	LJG

Hecho por:_____ Fecha: 14/11/13

Revisado por:_____ Fecha: 07/12/13

Autorizado por:_____ Fecha: 07/12/13

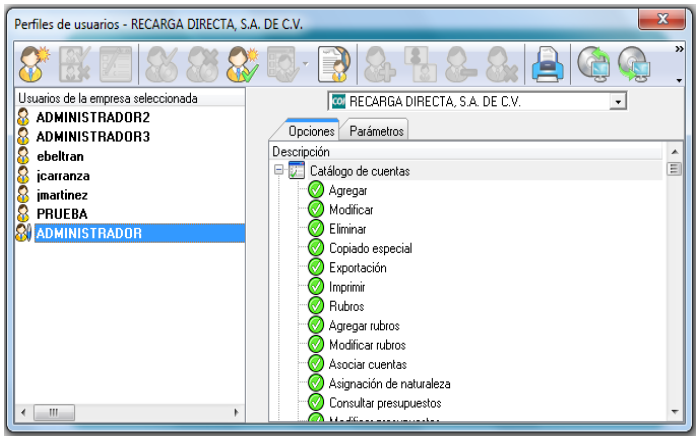
G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0	2012	PSS
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: SEGURIDAD DEL SISTEMA

Contenido: Solicitar acceso a la tabla de perfiles de usuario del sistema.

Se procedió a requerir del administrador del sistema un detalle de los usuarios actuales vigentes en el sistema ASPEL COI 6.0; como resultado se obtuvo la siguiente figura:



Conclusión: La entidad cuenta con 7 usuarios vigentes, los caracteres de identificación son a través de letras y vocales, mínimamente hay usuarios que se diferencian a través de números sucesivos.

PS1

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0	2012	PSS
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: SEGURIDAD DEL SISTEMA

Contenido: Revisar en los perfiles de usuario quienes son los autorizados para acceder a los campos de parametrización

Fueron revisados cada perfil de usuario y se prestó especial atención a la parte del perfil que establece los privilegios de parametrización, se logró determinar la siguiente figura:

Opciones usuarios	ADMINISTRADOR2	ADMINISTRADOR3	ebeltran	jcarranza	jmartinez	PRUEBA	Auxiliar	Capturista	Contador	Contralor	ADMINISTRADOR
⊟ Configuración	☑	☑	☐	☑	☐	☑	☐	☐	☑	☑	☑
⊟ Parámetros del sistema	☑	☑	☐	☑	☐	☑	☐	☐	☑	☑	☑
Configuración avanzada de base de datos	☑	☑	☐	☑	☐	☑	☐	☐	☑	☑	☑
Datos de la empresa	☑	☑	☐	☑	☐	☑	☐	☐	☑	☑	☑
⊟ Preferencias	☑	☑	☐	☑	☐	☑	☐	☐	☑	☑	☑
Barra de herramientas	☑	☑	☐	☑	☐	☑	☐	☐	☑	☑	☑
Perfiles de usuario	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Agregar empresa	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑

Conclusión: De los siete usuarios existen cinco que tienen privilegios de parametrización en el sistema, esto constituye un factor de riesgo TI relevante a la información financiera, ya que pueden ser modificados por varias personas en cualquier momento, se procederá a valorar este riesgo a través de una discusión con los miembros del equipo de trabajo de auditoría.

PS2

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0	2012	PSS
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: SEGURIDAD DEL SISTEMA

Contenido: Revisar en los perfiles de usuario si los privilegios establecidos están de acuerdo a los roles y responsabilidades del usuario.

Se hizo una revisión detallada de los roles que posee cada uno de los usuarios en la empresa, y fueron comparados a nivel de consulta con los privilegios que poseían en el sistema Aspel COI 6.0, el resultado de la revisión se resume en el siguiente cuadro esquemático:

Nombre de usuario	Perfil acorde a funciones
ADMINISTRADOR2	SI
ADMINISTRADOR3	SI
ebeltran	SI
jcarranza	NO
jmartinez	SI
PRUEBA	N/A
ADMINISTRADOR	SI

Conclusión: Existe un usuario que tiene acceso más allá de los necesarios para cumplir sus tareas encomendadas en la organización, además es notorio que la existencia del usuario "prueba" impide poder compararlo con algún puesto especifico, ya que no representa ninguna persona o cargo en la institución.

PS3

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0	2012	PSS
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: SEGURIDAD DEL SISTEMA

Contenido: Verifique cuantos administradores o súper usuarios del sistema existen.

Se hizo una inspección minuciosa de los privilegios globales que poseen los usuarios vigentes en el sistema, y se constató la siguiente información:

Nombre de usuario	¿Súper usuario?
ADMINISTRADOR2	SI
ADMINISTRADOR3	SI
ebeltran	NO
jcarranza	NO
jmartinez	NO
PRUEBA	SI
ADMINISTRADOR	SI

Conclusión: Al contar con más de un supe usuario la entidad se enfrenta al riesgo de cambios en el sistema no autorizados, acceso no autorizado a los datos procesados, etc. Existe una debilidad importante en la gestión de usuarios.

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0	2012	PSS
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: SEGURIDAD DEL SISTEMA

Contenido: Indague acerca de la política empresarial para establecer nombres de usuario, por ejemplo: nombre y apellido, primer letra del apellido y nombre completo, etc.

La política de la empresa para establecer nombres de usuario consiste en poner el primer carácter del primer nombre seguido del primer apellido del usuario. No hay excepciones.

Ejemplo:
Nombre completo de usuario: Héctor Armando Molina Rodríguez
Nombre de usuario: hmolina.

Conclusión: La entidad cuenta con un procedimiento para nombrar a todos los usuarios del sistema Aspel COI 6.0

PS5

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0	2012	PSS
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: SEGURIDAD DEL SISTEMA

Contenido: Verifique si los nombres de usuarios cumplen con la política de la empresa previamente establecida.

Se hizo una comparación entre los nombres de usuarios vigentes en el sistema y la política de nombres aprobada por la entidad, al hacerlo se obtuvo el siguiente resultado:

Nombre de usuario	Cumple política
ADMINISTRADOR2	NO
ADMINISTRADOR3	NO
ebeltran	SI
jcarranza	SI
jmartinez	SI
PRUEBA	NO
ADMINISTRADOR	NO

Conclusión: La entidad no cumple con la política de nombres en los usuarios, más de la mitad de los usuarios existentes no respetan los procedimientos aprobados por la administración TI.

PS6

ANEXO 8.2

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

PROGRAMA DE BITÁCORA DEL SISTEMA

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PBS

OBJETIVO: Indagar sobre la existencia, uso, funcionamiento y adecuación de la bitácora del sistema.

ALCANCE: Será revisada la bitácora del sistema de forma general.

No.	PROCEDIMIENTO	REF. CUEST	REF. PT	HECHO POR
1	Solicite acceso a la tabla de almacenamiento de la bitácora del sistema		BS1	O.A.M.
2	Solicite información a recursos humanos sobre los horarios laborales autorizados		BS2	O.A.M.
3	Haga un filtro de aquellas transacciones que se encuentre fuera de los horarios laborales establecidos		BS3	O.A.M.
4	Haga un filtro de aquellas transacciones que se encuentren en días no hábiles de trabajo		BS3	O.A.M.
5	Compare la tabla de perfiles de usuario y compruebe si existen usuarios que puedan editar la bitácora del sistema		BS4	O.A.M.
6	Realice una transacción de prueba con un usuario en particular y verifique si es almacenado en la bitácora su historial		BS5	O.A.M.

Hecho por:_____ Fecha: 14/11/13

Revisado por:_____ Fecha: 07/12/13

Autorizado por:_____ Fecha: 07/12/13

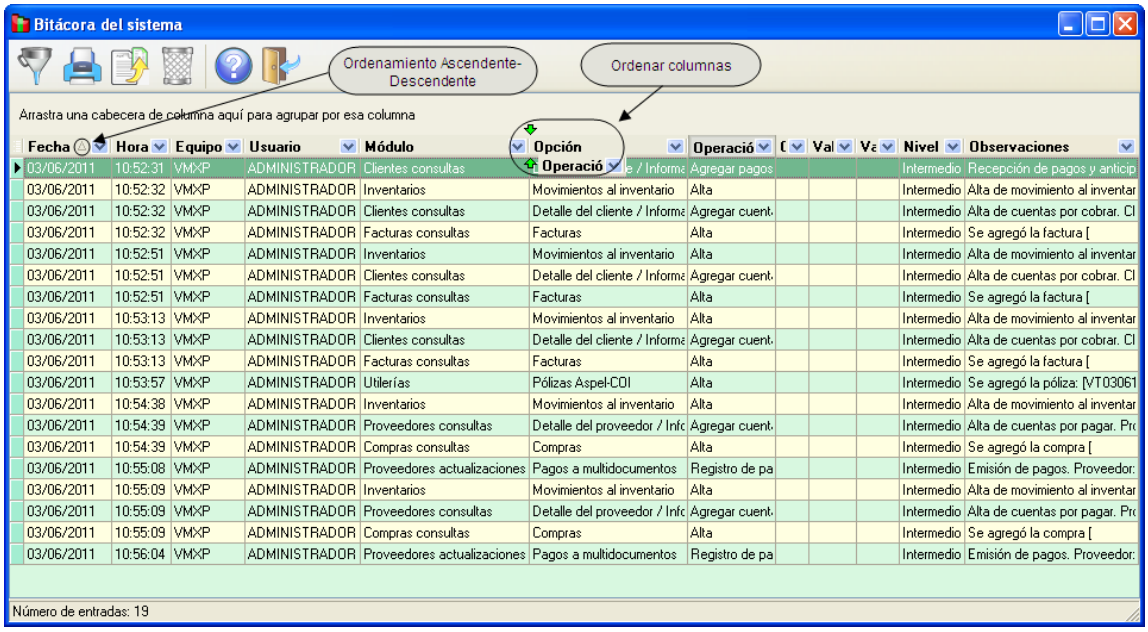
G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PBS
PREPARÓ: OAM	REVISÓ: MAG	

CÉDULA: BITÁCORA DEL SISTEMA

Contenido: Solicite acceso a la tabla de almacenamiento de la bitácora del sistema.

Se procedió a requerir del administrador del sistema la tabla de almacenamiento de la bitácora del sistema, sin embargo se nos mencionó que esta tabla esta encriptado para evitar modificaciones no autorizadas:



Fecha	Hora	Equipo	Usuario	Módulo	Opción	Operació	Nivel	Observaciones
03/06/2011	10:52:31	VMXP	ADMINISTRADOR	Clientes consultas	Operació	Agregar pagos	Intermedio	Recepción de pagos y anticip
03/06/2011	10:52:32	VMXP	ADMINISTRADOR	Inventarios	Movimientos al inventario	Alta	Intermedio	Alta de movimiento al inventar
03/06/2011	10:52:32	VMXP	ADMINISTRADOR	Clientes consultas	Detalle del cliente / Informa	Agregar cuent	Intermedio	Alta de cuentas por cobrar. Cl
03/06/2011	10:52:32	VMXP	ADMINISTRADOR	Facturas consultas	Facturas	Alta	Intermedio	Se agregó la factura [
03/06/2011	10:52:51	VMXP	ADMINISTRADOR	Inventarios	Movimientos al inventario	Alta	Intermedio	Alta de movimiento al inventar
03/06/2011	10:52:51	VMXP	ADMINISTRADOR	Clientes consultas	Detalle del cliente / Informa	Agregar cuent	Intermedio	Alta de cuentas por cobrar. Cl
03/06/2011	10:52:51	VMXP	ADMINISTRADOR	Facturas consultas	Facturas	Alta	Intermedio	Se agregó la factura [
03/06/2011	10:53:13	VMXP	ADMINISTRADOR	Inventarios	Movimientos al inventario	Alta	Intermedio	Alta de movimiento al inventar
03/06/2011	10:53:13	VMXP	ADMINISTRADOR	Clientes consultas	Detalle del cliente / Informa	Agregar cuent	Intermedio	Alta de cuentas por cobrar. Cl
03/06/2011	10:53:13	VMXP	ADMINISTRADOR	Facturas consultas	Facturas	Alta	Intermedio	Se agregó la factura [
03/06/2011	10:53:57	VMXP	ADMINISTRADOR	Utilerías	Pólizas Aspel-COI	Alta	Intermedio	Se agregó la póliza: [VT03061
03/06/2011	10:54:38	VMXP	ADMINISTRADOR	Inventarios	Movimientos al inventario	Alta	Intermedio	Alta de movimiento al inventar
03/06/2011	10:54:39	VMXP	ADMINISTRADOR	Proveedores consultas	Detalle del proveedor / Infc	Agregar cuent	Intermedio	Alta de cuentas por pagar. Pr
03/06/2011	10:54:39	VMXP	ADMINISTRADOR	Compras consultas	Compras	Alta	Intermedio	Se agregó la compra [
03/06/2011	10:55:08	VMXP	ADMINISTRADOR	Proveedores actualizaciones	Pagos a multidocumentos	Registro de pa	Intermedio	Emisión de pagos. Proveedor:
03/06/2011	10:55:09	VMXP	ADMINISTRADOR	Inventarios	Movimientos al inventario	Alta	Intermedio	Alta de movimiento al inventar
03/06/2011	10:55:09	VMXP	ADMINISTRADOR	Proveedores consultas	Detalle del proveedor / Infc	Agregar cuent	Intermedio	Alta de cuentas por pagar. Pr
03/06/2011	10:55:09	VMXP	ADMINISTRADOR	Compras consultas	Compras	Alta	Intermedio	Se agregó la compra [
03/06/2011	10:56:04	VMXP	ADMINISTRADOR	Proveedores actualizaciones	Pagos a multidocumentos	Registro de pa	Intermedio	Emisión de pagos. Proveedor:

CP: Contenido de la cédula preparado por el cliente.

Conclusión: Se pudo observar en la bitácora del sistema que contiene al menos los elementos mínimos importantes.

BS1

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PBS
PREPARÓ: OAM	REVISÓ: MAG	

CÉDULA: BITÁCORA DEL SISTEMA

Contenido: Solicite información a recursos humanos sobre los horarios laborales autorizados.

Se solicitó al gerente de recursos humanos, el detalle de horas laborales, que incluya días hábiles, días no hábiles.

Narrativa de los horarios de trabajo:

"En la empresa se respeta el horario de trabajo establecido en el contrato individual de trabajo, nuestro horario regular es de 8:00 a.m. a 5:00 p.m., en algunos cosas las personas del área administrativa como contabilidad, cuentas por cobrar y el gerente financiero, laboran hasta las 9:00 p.m., sin embargo estos horarios son autorizados previamente y se lleva un control del horario de ese personal.

Por política de la empresa, ningún empleado puede trabajar en días no hábiles como Domingo, o los decretados como asueto por la honorable Asamblea Legislativa."

: Completado con fuente de información de la compañía

Conclusión: Las políticas de entrada y salida de personal están por escrito, los usuarios que se extienden fuera de su horario de normal trabajo deben solicitar autorización.

BS2

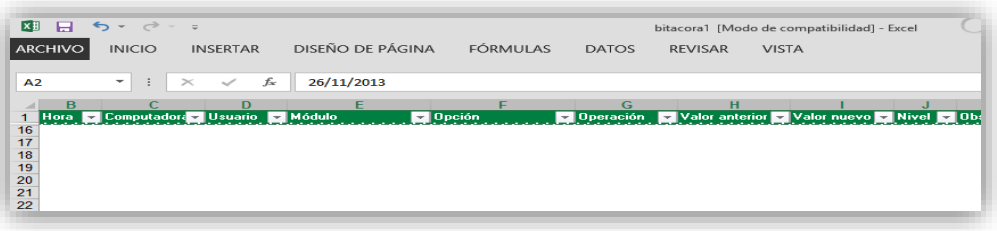
G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PBS
PREPARÓ: OAM	REVISÓ: MAG	

CÉDULA: BITÁCORA DEL SISTEMA

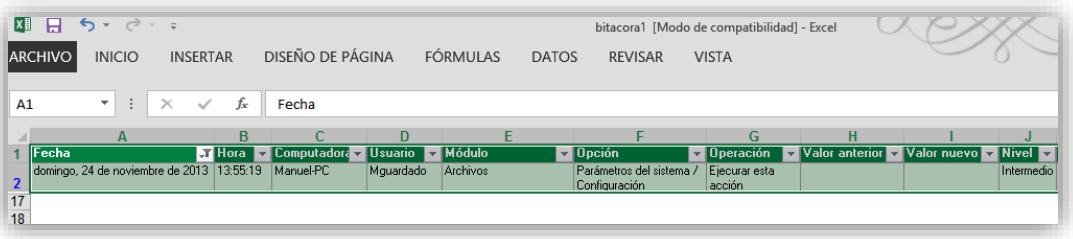
Contenido: Haga un filtro de aquellas transacciones que se encuentre fuera de los horarios del día y de los días no hábiles:

a) Haga un filtro de aquellas transacciones que se encuentre fuera de los horarios laborales establecidos:



Resultado: ningún valor encontrado.

b) Haga un filtro de aquellas transacciones que se encuentren en días no hábiles de trabajo.



Resultado: Se encontraron transacciones de día no hábil como domingo.

Conclusión: En la bitácora del sistema se apreció que existen transacciones fuera del horario normal de trabajo.

BS3

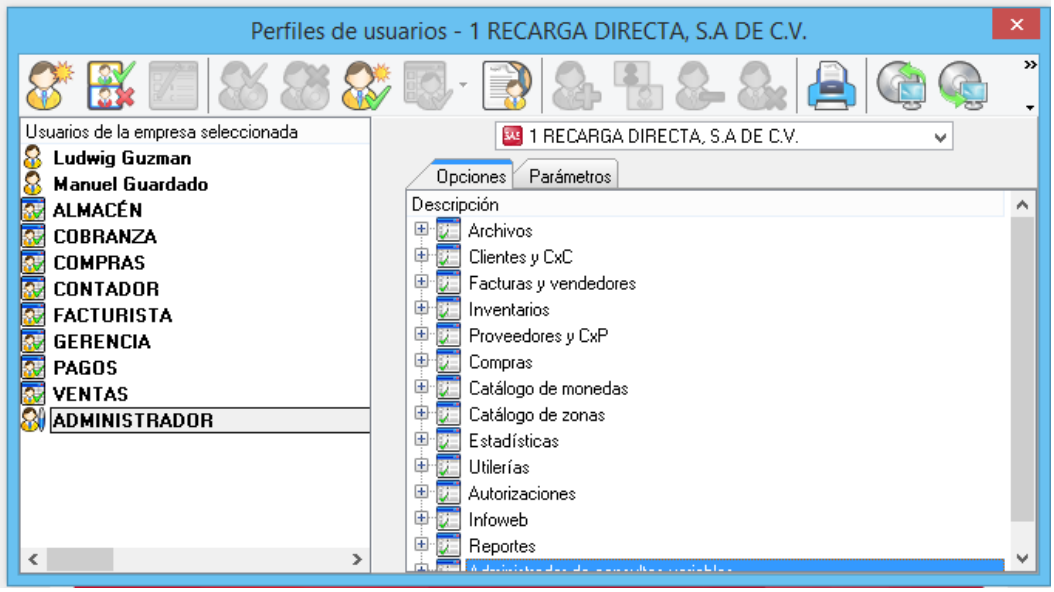
G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PBS
PREPARÓ: OAM	REVISÓ: MAG	

CÉDULA: BITÁCORA DEL SISTEMA

Contenido: Verifique en la tabla de perfiles de usuario y compruebe si existen usuarios con acceso a editar la bitácora del sistema.

Se verificó los perfiles de usuario del administrador del sistema, verificando las opciones disponibles accesibles y no accesibles:



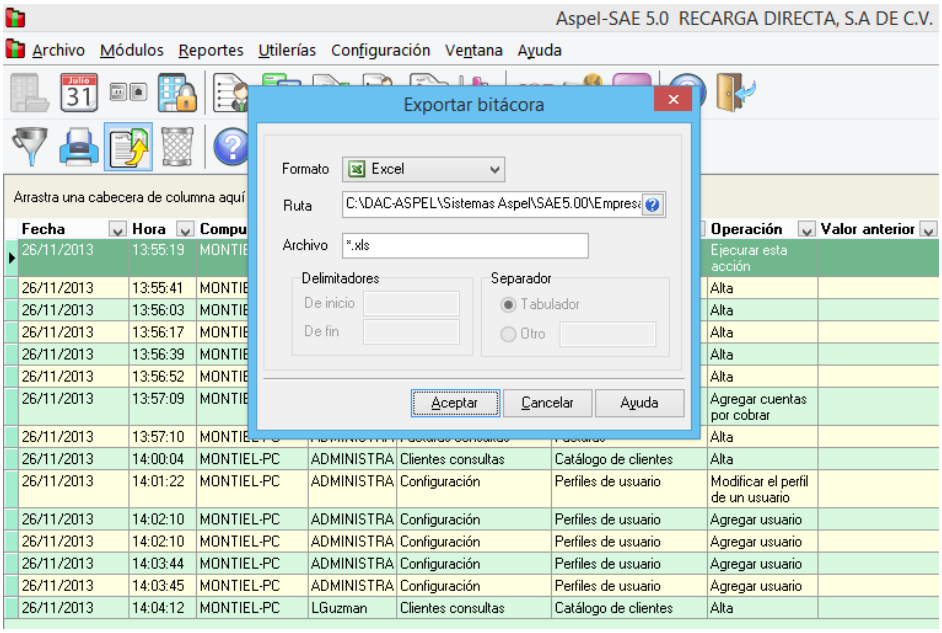
No se observa ninguna opción, relevante a editar la bitacora, sin embargo consultamos si es exportable a excel y verificamos la opción disponible en el sistema como sigue:

BS4

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PBS
PREPARÓ: OAM	REVISÓ: MAG	

CÉDULA: BITÁCORA DEL SISTEMA



Se observó que la bitácora del sistema es exportable a Excel, esta utilidad puede facilitar su manipulación.

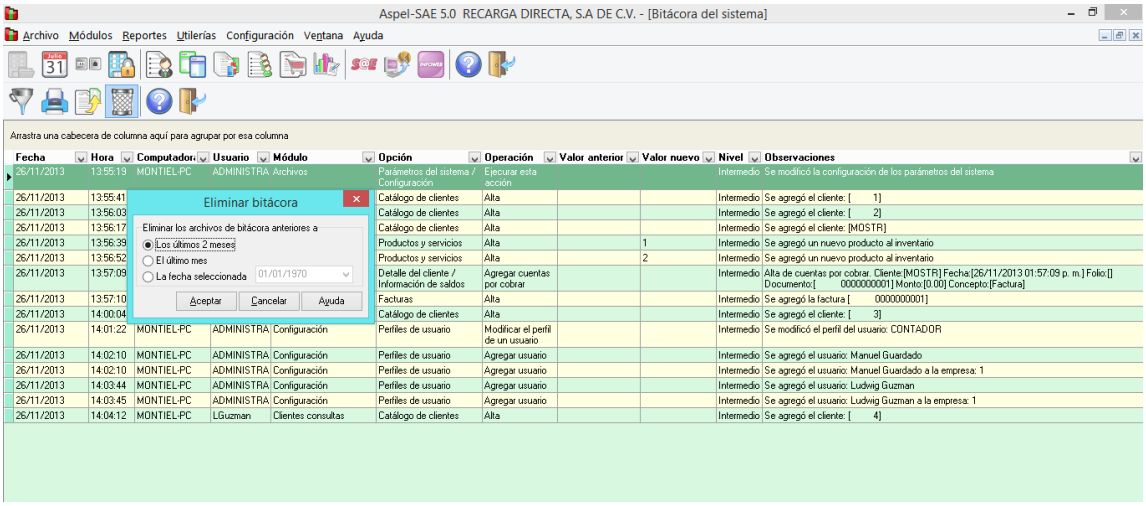
Sin embargo se apreció que la información que origina la bitácora se puede eliminar por cada módulo:

BS4

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PBS
PREPARÓ: OAM	REVISÓ: MAG	

CÉDULA: BITÁCORA DEL SISTEMA



Fecha	Hora	Computador	Usuario	Módulo	Opción	Operación	Valor anterior	Valor nuevo	Nivel	Observaciones
26/11/2013	13:55:19	MONTIEL-PC	ADMINISTRA	Archivos	Parámetros del sistema / Configuración	Ejecurar esta acción			Intermedio	Se modificó la configuración de los parámetros del sistema
26/11/2013	13:55:41				Catálogo de clientes	Alta			Intermedio	Se agregó el cliente: [1]
26/11/2013	13:56:03				Catálogo de clientes	Alta			Intermedio	Se agregó el cliente: [2]
26/11/2013	13:56:17				Catálogo de clientes	Alta			Intermedio	Se agregó el cliente: [MOSTR]
26/11/2013	13:56:39				Productos y servicios	Alta		1	Intermedio	Se agregó un nuevo producto al inventario
26/11/2013	13:56:52				Productos y servicios	Alta		2	Intermedio	Se agregó un nuevo producto al inventario
26/11/2013	13:57:09				Detalle del cliente / Información de saldos	Agregar cuentas por cobrar			Intermedio	Alta de cuentas por cobrar. Cliente:[MOSTR] Fecha:[26/11/2013 01:57:09 p. m.] Folio:[] Documento:[0000000001] Monto:[0.00] Concepto:[Factura]
26/11/2013	13:57:10				Facturas	Alta			Intermedio	Se agregó la factura [0000000001]
26/11/2013	14:00:04				Catálogo de clientes	Alta			Intermedio	Se agregó el cliente: [3]
26/11/2013	14:01:22	MONTIEL-PC	ADMINISTRA	Configuración	Perfiles de usuario	Modificar el perfil de un usuario			Intermedio	Se modificó el perfil del usuario: CONTADOR
26/11/2013	14:02:10	MONTIEL-PC	ADMINISTRA	Configuración	Perfiles de usuario	Agregar usuario			Intermedio	Se agregó el usuario: Manuel Guardado
26/11/2013	14:02:10	MONTIEL-PC	ADMINISTRA	Configuración	Perfiles de usuario	Agregar usuario			Intermedio	Se agregó el usuario: Manuel Guardado a la empresa: 1
26/11/2013	14:03:44	MONTIEL-PC	ADMINISTRA	Configuración	Perfiles de usuario	Agregar usuario			Intermedio	Se agregó el usuario: Ludwig Guzman
26/11/2013	14:03:45	MONTIEL-PC	ADMINISTRA	Configuración	Perfiles de usuario	Agregar usuario			Intermedio	Se agregó el usuario: Ludwig Guzman a la empresa: 1
26/11/2013	14:04:12	MONTIEL-PC	LGuzman	Clientes consultas	Catálogo de clientes	Alta			Intermedio	Se agregó el cliente: [4]

Conclusión: Dentro de las opciones generadas por los perfiles de usuario, la bitácora no está disponible para su modificación, sin embargo es posible exportarla a Excel y reformatearla, así como eliminarla directamente por medio de un usuario autorizado.

BS4

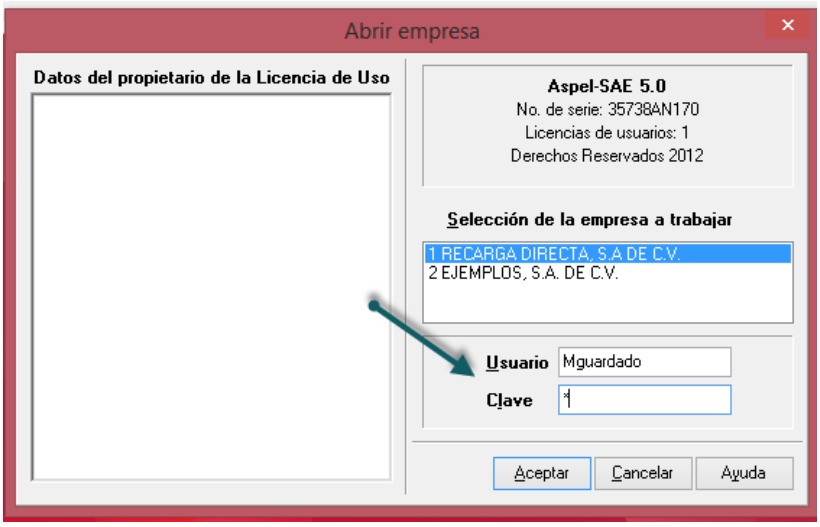
G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PBS
PREPARÓ: OAM	REVISÓ: MAG	

CÉDULA: BITÁCORA DEL SISTEMA

Contenido: Realice una transacción de prueba con un usuario en particular y verifique si es almacenado en la bitácora su historial.

Se inició sesión con el usuario "Mguardado";

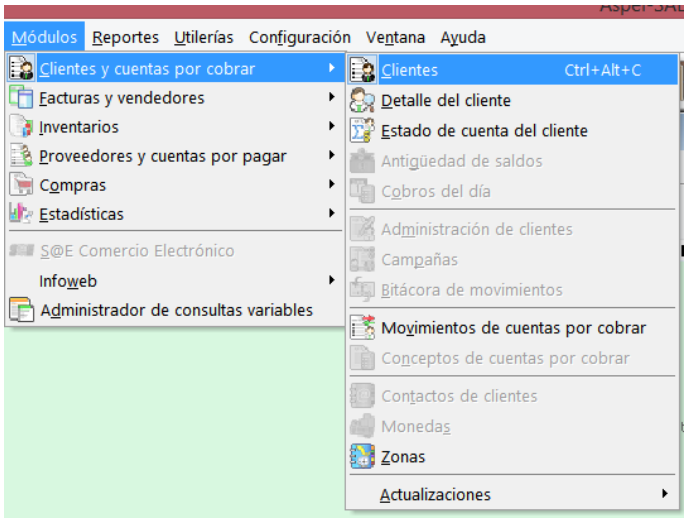


Se procedió a ingresar al módulo de cuentas por cobrar.

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PBS
PREPARÓ: OAM	REVISÓ: MAG	

CÉDULA: BITÁCORA DEL SISTEMA



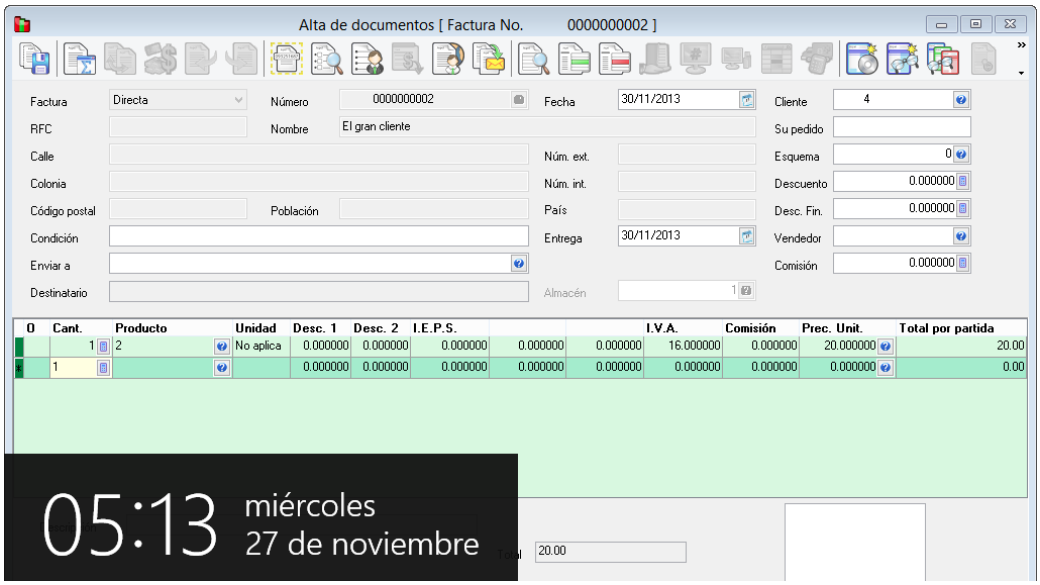
Se procedió a dar de alta un documento, una factura por $20.00, en fecha 27-11-2013 tal como lo muestra la prueba.

BS5

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PBS
PREPARÓ: OAM	REVISÓ: MAG	

CÉDULA: BITÁCORA DEL SISTEMA

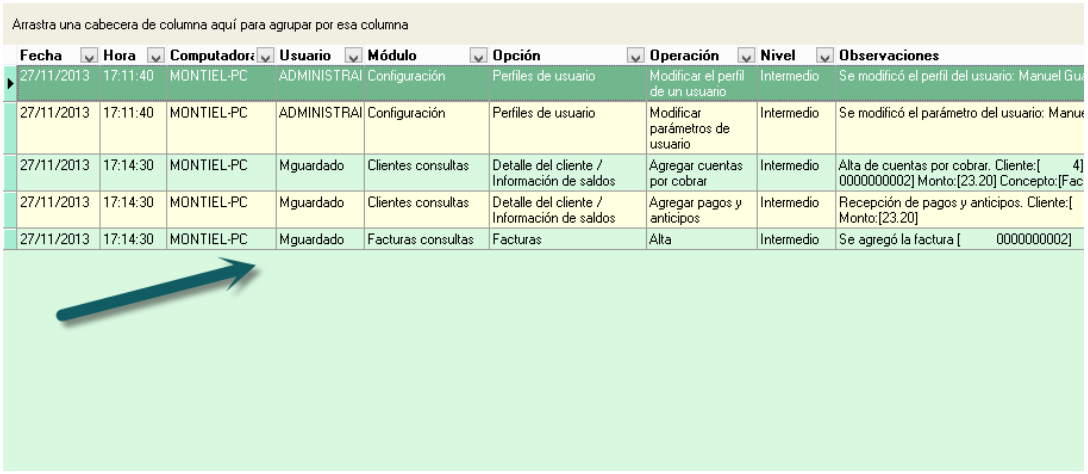


Posteriormente, se verifico si el documento quedo registrado

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PBS
PREPARÓ: OAM	REVISÓ: MAG	

CÉDULA: BITÁCORA DEL SISTEMA



Arrastra una cabecera de columna aquí para agrupar por esa columna

Fecha	Hora	Computador	Usuario	Módulo	Opción	Operación	Nivel	Observaciones
27/11/2013	17:11:40	MONTIEL-PC	ADMINISTRAI	Configuración	Perfiles de usuario	Modificar el perfil de un usuario	Intermedio	Se modificó el perfil del usuario: Manuel Gu
27/11/2013	17:11:40	MONTIEL-PC	ADMINISTRAI	Configuración	Perfiles de usuario	Modificar parámetros de usuario	Intermedio	Se modificó el parámetro del usuario: Manu
27/11/2013	17:14:30	MONTIEL-PC	Mguardado	Clientes consultas	Detalle del cliente / Información de saldos	Agregar cuentas por cobrar	Intermedio	Alta de cuentas por cobrar. Cliente:[4] 0000000002] Monto:[23.20] Concepto:[Fac
27/11/2013	17:14:30	MONTIEL-PC	Mguardado	Clientes consultas	Detalle del cliente / Información de saldos	Agregar pagos y anticipos	Intermedio	Recepción de pagos y anticipos. Cliente:[Monto:[23.20]
27/11/2013	17:14:30	MONTIEL-PC	Mguardado	Facturas consultas	Facturas	Alta	Intermedio	Se agregó la factura [0000000002]

Se verificó que la factura 002, con fecha 27-11-2013 fue correctamente registrada por la bitácora del sistema.

Conclusión: La bitácora del sistema registra los eventos importantes de modificación, adición y eliminación de operaciones en el sistema.

BS5

ANEXO 8.3

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

PROGRAMA DE VALORES PARAMETRIZABLES

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PVP

OBJETIVO: Conocer las políticas relativas a datos parametrizables del sistema contable informático y su adecuación con respecto a los requerimientos legales y normativos aplicables.

ALCANCE: Se examinarán todos los campos con opciones de parametrización que posea el sistema.

N°	Procedimiento	Ref. Cuest.	Ref. P/T	Hecho por
1	Solicite acceso al sistema y verifique todos los campos con opciones de parametrización, tales como, depreciación, amortización, retenciones de IVA, porcentajes de impuestos, estimaciones por incobrabilidad y cuentas contables enlazadas a los módulos.		VP1	LJG
2	Compare la tabla de perfiles de usuario y compruebe si existen usuarios que puedan editar los valores parametrizados anteriormente.		VP2	LJG
3	Solicite las políticas contables de la entidad relativas a depreciación, amortización, estimaciones por incobrabilidad.		VP3	LJG
4	Compare las políticas anteriores con los valores parametrizados en el sistema.		VP4	LJG
5	Realice una transacción de prueba con un usuario particular y verifique si es posible registrar transacciones en un periodo cerrado y o no habilitado.		VP5	LJG
6	Utilice el perfil de usuario del administrador del sistema e intente modificar transacciones en aspectos tales como, montos y fechas.		VP6	LJG

Hecho por:_____ Fecha: 14/11/13

Revisado por:_____ Fecha: 07/12/13

Autorizado por:_____ Fecha: 07/12/13

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

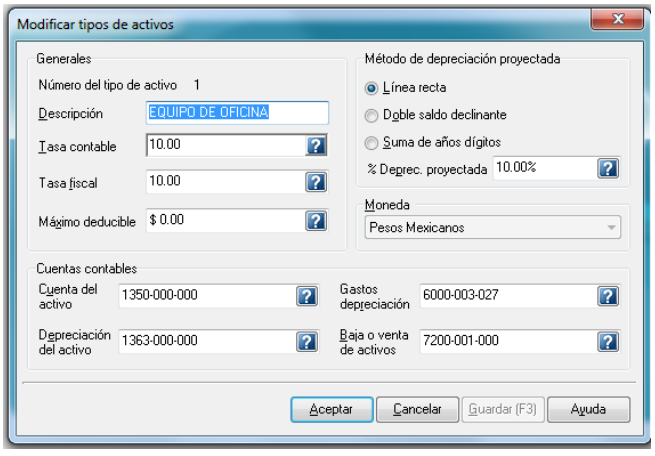
CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PVP
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: VALORES PARAMETRIZABLES

Contenido: Solicite acceso al sistema y verifique todos los campos con opciones de parametrización, tales como, depreciación, amortización, retenciones de IVA, porcentajes de impuestos, estimaciones por incobrabilidad y cuentas contables enlazadas a los módulos.

Depreciaciones

Se solicitó acceso al sistema para verificar si la depreciación es parametrizable, se obtuvo el siguiente resultado:



Amortizaciones

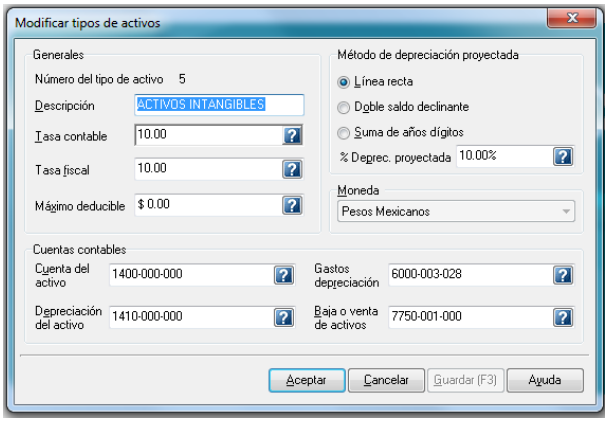
Se solicitó acceso al sistema para verificar si las amortizaciones son parametrizables, se obtuvo el siguiente resultado:

VP1

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PVP
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: VALORES PARAMETRIZABLES



Retenciones IVA

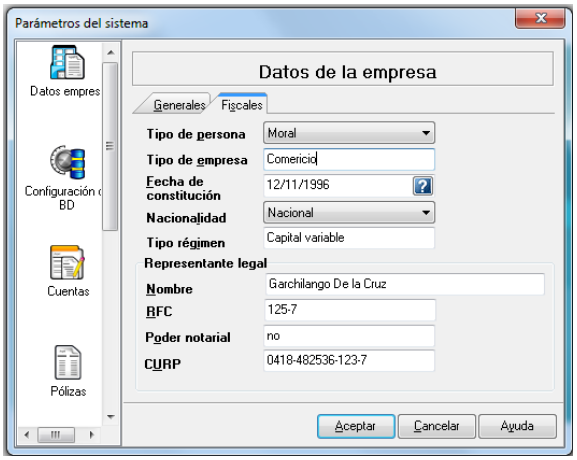
Se solicitó acceso al sistema para verificar si las retenciones y percepciones del IVA son parametrizables, y según comentarios de la administración, estos porcentajes no pueden ser configurados debido a que el sistema no contempla esta figura fiscal.

Porcentajes de impuestos

Al examinar los valores parametrizables relativos a impuestos se pudo constatar que no es posible configurar las tasas de los impuestos IVA e impuesto sobre la renta. Los únicos campos de configuración son los descritos en el siguiente esquema:

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PVP
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: VALORES PARAMETRIZABLES



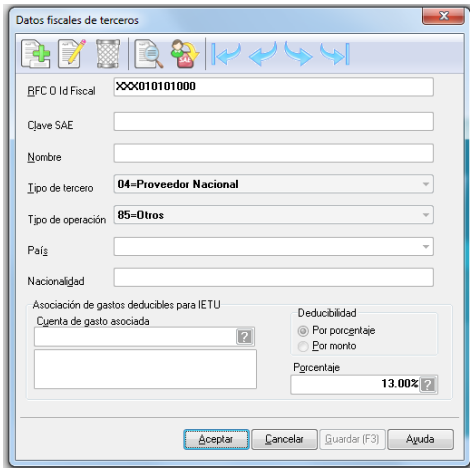
Con respecto a los proveedores, es posible configurar una tasa de impuesto (IVA) de acuerdo al tipo de proveedor que se trate, tal detalle es mostrado a continuación:

VP1

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PVP
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: VALORES PARAMETRIZABLES



El sistema provee además de un parámetro que permite poder establecer los tipos de impuesto y en que clases de transacciones realizar, estos conceptos están parametrizados en el siguiente recuadro:

VP1

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PVP
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: VALORES PARAMETRIZABLES

Estimaciones por incobrabilidad

Se solicitó acceso al sistema de los parámetros para el cálculo de las cuentas incobrables, la administración manifiesta que el sistema no tiene ningún campo habilitado para la realización de este tipo de configuración

Conclusión: La entidad posee algunos de los principales conceptos parametrizables, sin embargo, se ha observado que esta información puede ser modificada a discreción por parte de los tres administradores del sistema, hecho que constituye un factor de riesgo importante a considerar.

VP1

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

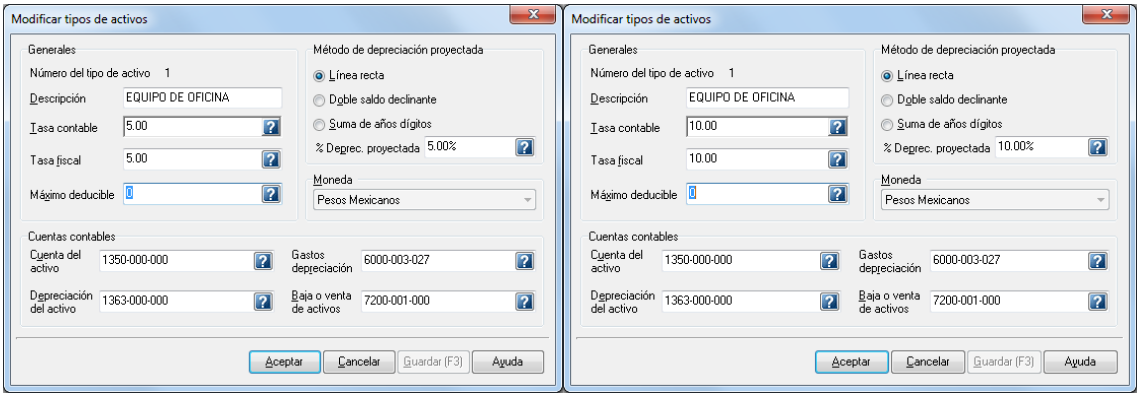
CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PVP
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: VALORES PARAMETRIZABLES

Contenido: Compare la tabla de perfiles de usuario y compruebe si existen usuarios que puedan editar los valores parametrizados anteriormente.

Depreciaciones

Se utilizó el usuario jcarranza para determinar si los valores parametrizados de depreciación podían ser modificados, el resultado fue positivo, cambiándose de una tasa del 10% al 5%, así:



Esto constituye un grave problema de parametrización.

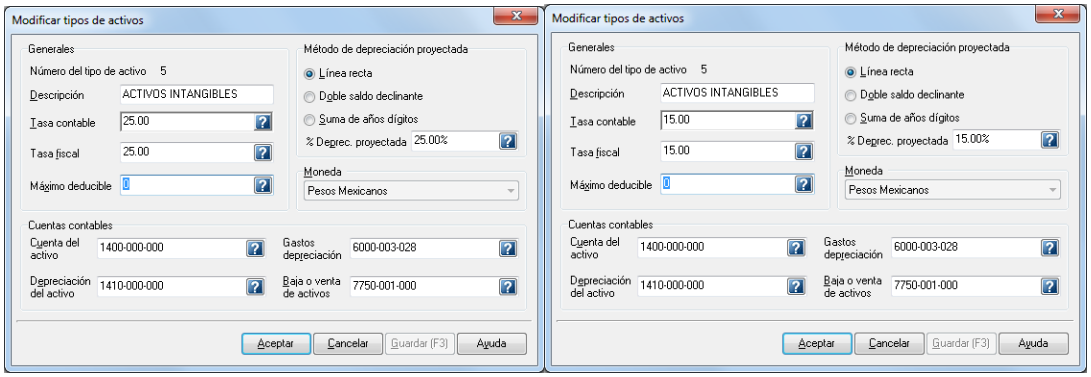
Amortizaciones

Siempre con el mismo usuario (jcarranza) se le pidió que intentara modificar los parámetros establecidos para la amortización de los activos intangibles, el resultado fue positivo y se logró cambiar de un 25% hacia un 15%, así:

VP2

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PVP
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: VALORES PARAMETRIZABLES



Esto constituye otro grave problema de parametrización en cuanto a la amortización de los intangibles manejados por la entidad.

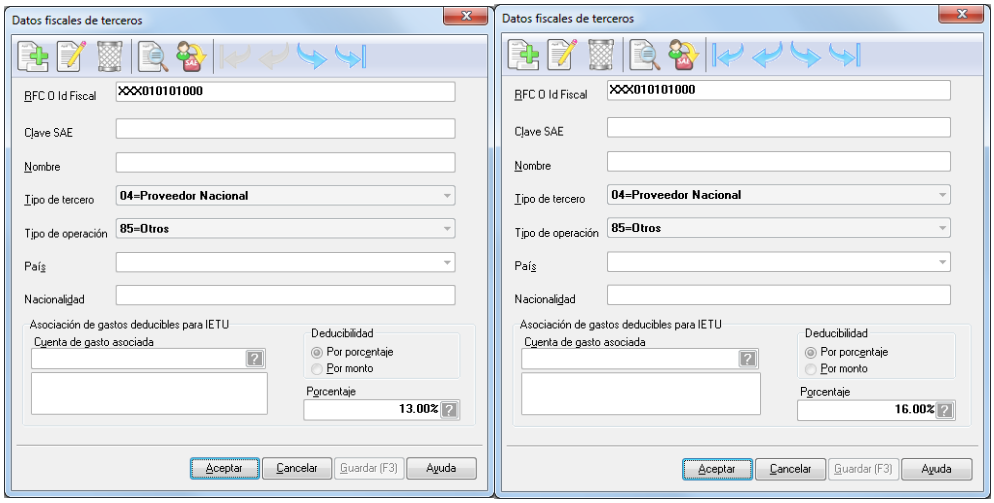
Por cuanto los valores de retención y percepción del impuesto IVA y la estimación de cuentas incobrables no están contempladas dentro de los parámetros de la entidad, fueron obviados estos procedimientos, paso seguido se procedió con la parametrización de las tasas de impuestos IVA.

Al usuario jcarranza se le indicó que tratara de modificar la tasa del impuesto IVA parametrizados en el sistema, como resultado, se pudo cambiar sin ningún problema, de un 13% al 16%, así:

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PVP
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: VALORES PARAMETRIZABLES



Los impuestos pudieron ser modificados en razón de su tasa.

Conclusión: A pesar que el sistema tiene campos directos para realizar una parametrización eficiente, se posee la deficiencia de control TI en cuanto a que estos valores pueden ser cambiados sin previo consentimiento del administrador de sistemas.

VP2

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PVP
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: VALORES PARAMETRIZABLES

Contenido: Solicite las políticas contables de la entidad relativas a depreciación, amortización, estimaciones por incobrabilidad.

Las políticas contables para la depreciación de activos son las siguientes:

Vehículos	6 años	equivalente al 20% anual
Edificio	20 años	equivalente al 5% anual
Mobiliario	4 años	equivalente al 25% anual
Otros	2 años	equivalente al 50% anual

Las políticas para la amortización de los activos intangibles son los siguientes:

Amortización	4 años	equivalente al 25% anual

La política de estimación por incobrabilidad es realizada en un 6% del saldo de clientes a la fecha de cada cierre mensual contable

Conclusión: La entidad tiene establecidas políticas contables relacionadas con la depreciación, amortización e incobrabilidad. Respetan los requerimientos legales y técnicos aplicables.

VP3

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

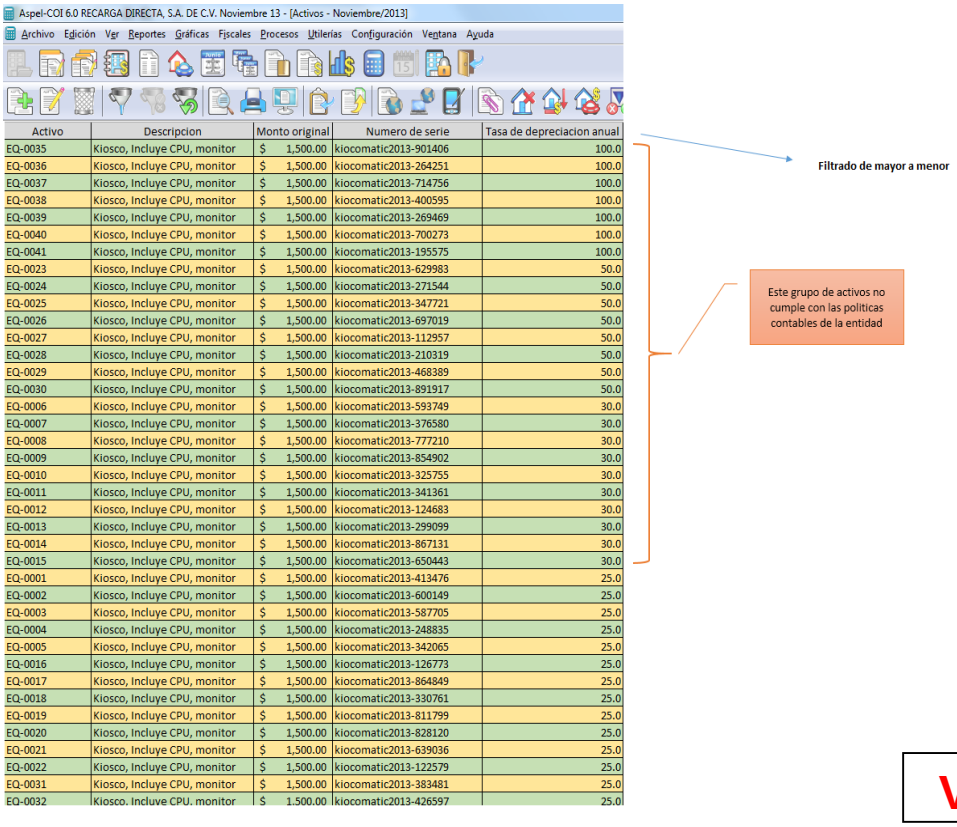
CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PVP
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: VALORES PARAMETRIZABLES

Contenido: Compare las políticas anteriores con los valores parametrizados en el sistema.

Depreciaciones

Para comparar las políticas parametrizados fue solicitado al gerente de informática la base de datos actual correspondiente al activo más representativo de la entidad, el cual corresponde a los kioscos, con la base de datos se hizo un filtro en la columna “tasa depreciación anual” y el resultado fue el siguiente:



Activo	Descripcion	Monto original	Numero de serie	Tasa de depreciacion anual
EQ-0035	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-901406	100.0
EQ-0036	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-264251	100.0
EQ-0037	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-714756	100.0
EQ-0038	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-400595	100.0
EQ-0039	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-269469	100.0
EQ-0040	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-700273	100.0
EQ-0041	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-195575	100.0
EQ-0023	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-629983	50.0
EQ-0024	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-271544	50.0
EQ-0025	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-347721	50.0
EQ-0026	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-697019	50.0
EQ-0027	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-112957	50.0
EQ-0028	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-210319	50.0
EQ-0029	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-468389	50.0
EQ-0030	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-891917	50.0
EQ-0006	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-593749	30.0
EQ-0007	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-376580	30.0
EQ-0008	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-777210	30.0
EQ-0009	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-854902	30.0
EQ-0010	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-325755	30.0
EQ-0011	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-341361	30.0
EQ-0012	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-124683	30.0
EQ-0013	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-299099	30.0
EQ-0014	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-867131	30.0
EQ-0015	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-650443	30.0
EQ-0001	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-413476	25.0
EQ-0002	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-600149	25.0
EQ-0003	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-587705	25.0
EQ-0004	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-248835	25.0
EQ-0005	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-342065	25.0
EQ-0016	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-126773	25.0
EQ-0017	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-864849	25.0
EQ-0018	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-330761	25.0
EQ-0019	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-811799	25.0
EQ-0020	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-828120	25.0
EQ-0021	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-639036	25.0
EQ-0022	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-122579	25.0
EQ-0031	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-383481	25.0
EQ-0032	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-426597	25.0

VP4

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PVP
PREPARÓ: LJG	REVISÓ: OAM	

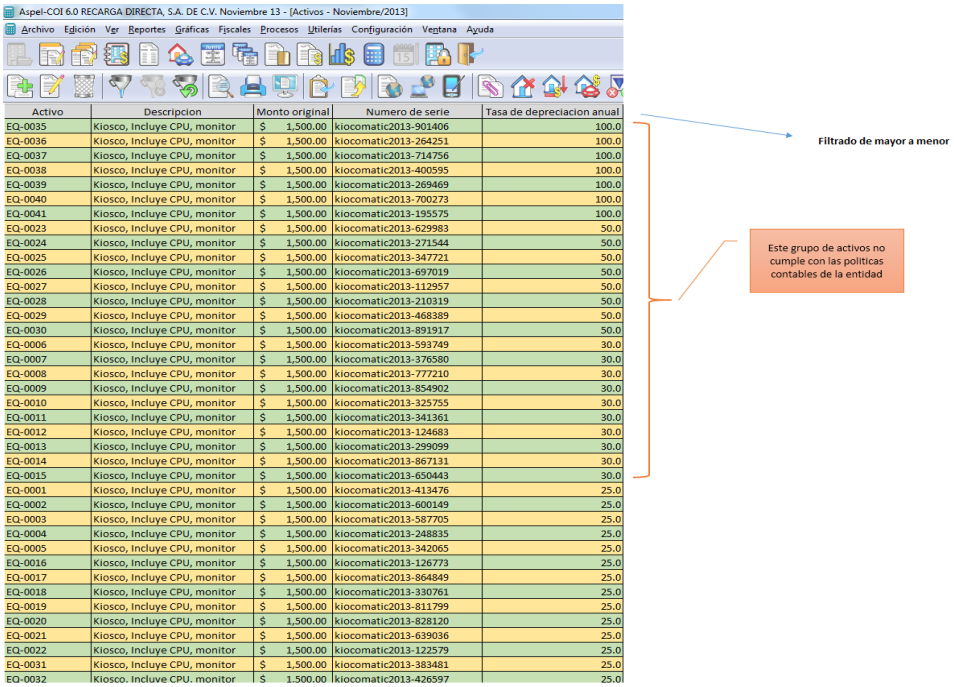
CÉDULA: VALORES PARAMETRIZABLES

Se pudo evidenciar que existen muchos activos "kioscos" cuyas tasas de depreciación no corresponden a lo establecido en las políticas contables de la entidad, además, están por encima de lo que ley establece para deducir, ya que puede observarse que existen 8 kioscos que tienen una tasa muy por encima de lo permitido por el art. 30 de la ley de ISR.

Depreciaciones

Para comparar las políticas parametrizados fue solicitado al gerente de informática la base de datos actual correspondiente al activo más representativo de la entidad, el cual corresponde a los kioscos, con la base

de datos se hizo un filtro en la columna “tasa depreciación anual” y el resultado fue el siguiente:



Activo	Descripcion	Monto original	Numero de serie	Tasa de depreciacion anual
EQ-0035	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-901406	100.0
EQ-0036	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-264251	100.0
EQ-0037	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-714756	100.0
EQ-0038	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-400595	100.0
EQ-0039	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-269469	100.0
EQ-0040	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-700273	100.0
EQ-0041	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-195575	100.0
EQ-0023	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-629983	50.0
EQ-0024	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-271544	50.0
EQ-0025	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-347721	50.0
EQ-0026	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-697019	50.0
EQ-0027	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-112957	50.0
EQ-0028	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-210319	50.0
EQ-0029	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-468389	50.0
EQ-0030	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-891917	50.0
EQ-0006	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-593749	30.0
EQ-0007	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-376580	30.0
EQ-0008	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-777210	30.0
EQ-0009	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-854902	30.0
EQ-0010	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-325755	30.0
EQ-0011	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-341361	30.0
EQ-0012	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-124683	30.0
EQ-0013	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-299099	30.0
EQ-0014	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-867131	30.0
EQ-0015	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-650443	30.0
EQ-0001	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-413476	25.0
EQ-0002	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-600149	25.0
EQ-0003	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-587705	25.0
EQ-0004	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-248835	25.0
EQ-0005	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-342065	25.0
EQ-0016	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-126773	25.0
EQ-0017	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-864849	25.0
EQ-0018	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-330761	25.0
EQ-0019	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-811799	25.0
EQ-0020	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-828120	25.0
EQ-0021	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-639036	25.0
EQ-0022	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-122579	25.0
EQ-0031	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-383481	25.0
EQ-0032	Kiosco, Incluye CPU, monitor	$ 1,500.00	kiocomatic2013-426597	25.0

CÉDULA: VALORES PARAMETRIZABLES

Se pudo evidenciar que existen muchos activos “kioscos” cuyas tasas de depreciación no corresponden a lo establecido en las políticas contables de la entidad, además, están por encima de lo que ley establece para deducir, ya que puede observarse que existen 8 kioscos que tienen una tasa muy por encima de lo permitido por el art. 30 de la ley de ISR

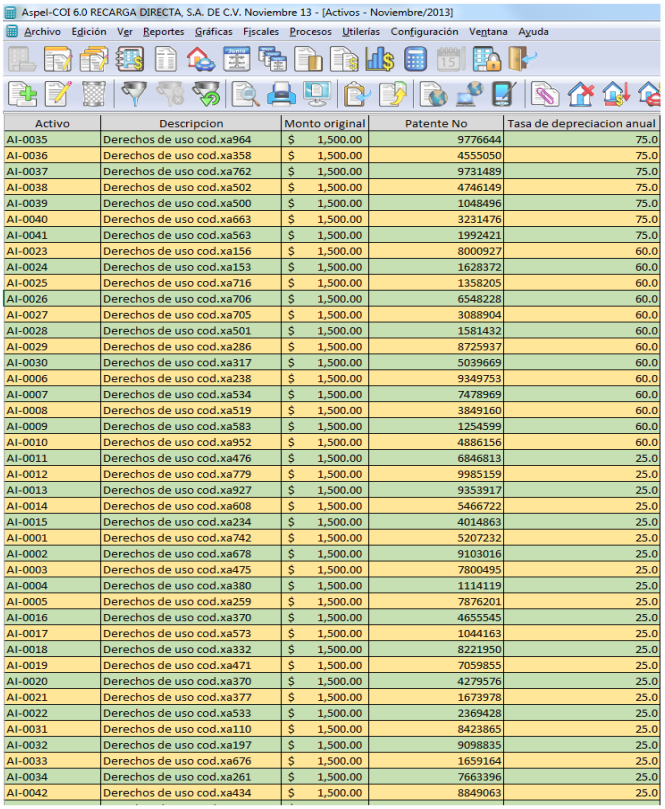
Amortizaciones

Actualmente la entidad posee activos intangibles que corresponden a derechos para hacer uso del sistema kioscos al momento de vender sus recargas de saldo y de paquetes de datos, en tal sentido existe uno para cada municipio en donde se haya establecido el kiosco. Para comparar las tasas de amortización según políticas, se solicitó al departamento de informática que extrajeran la base de datos de todos los intangibles reconocidos en contabilidad, al filtrar la columna "tasa de amortización anual, se encontró lo siguiente:

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	**PERIODO**	**VP4**
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	**2012**	**PVP**
PREPARÓ: LJG	**REVISÓ: OAM**	

CÉDULA: VALORES PARAMETRIZABLES



Activo	Descripcion	Monto original	Patente No	Tasa de depreciacion anual
AI-0035	Derechos de uso cod.xa964	$ 1,500.00	9776644	75.0
AI-0036	Derechos de uso cod.xa358	$ 1,500.00	4555050	75.0
AI-0037	Derechos de uso cod.xa762	$ 1,500.00	9731489	75.0
AI-0038	Derechos de uso cod.xa502	$ 1,500.00	4746149	75.0
AI-0039	Derechos de uso cod.xa500	$ 1,500.00	1048496	75.0
AI-0040	Derechos de uso cod.xa663	$ 1,500.00	3231476	75.0
AI-0041	Derechos de uso cod.xa563	$ 1,500.00	1992421	75.0
AI-0023	Derechos de uso cod.xa156	$ 1,500.00	8000927	60.0
AI-0024	Derechos de uso cod.xa153	$ 1,500.00	1628372	60.0
AI-0025	Derechos de uso cod.xa716	$ 1,500.00	1358205	60.0
AI-0026	Derechos de uso cod.xa706	$ 1,500.00	6548228	60.0
AI-0027	Derechos de uso cod.xa705	$ 1,500.00	3088904	60.0
AI-0028	Derechos de uso cod.xa501	$ 1,500.00	1581432	60.0
AI-0029	Derechos de uso cod.xa286	$ 1,500.00	8725937	60.0
AI-0030	Derechos de uso cod.xa317	$ 1,500.00	5039669	60.0
AI-0006	Derechos de uso cod.xa238	$ 1,500.00	9349753	60.0
AI-0007	Derechos de uso cod.xa534	$ 1,500.00	7478969	60.0
AI-0008	Derechos de uso cod.xa519	$ 1,500.00	3849160	60.0
AI-0009	Derechos de uso cod.xa583	$ 1,500.00	1254599	60.0
AI-0010	Derechos de uso cod.xa952	$ 1,500.00	4886156	60.0
AI-0011	Derechos de uso cod.xa476	$ 1,500.00	6846813	25.0
AI-0012	Derechos de uso cod.xa779	$ 1,500.00	9985159	25.0
AI-0013	Derechos de uso cod.xa927	$ 1,500.00	9353917	25.0
AI-0014	Derechos de uso cod.xa608	$ 1,500.00	5466722	25.0
AI-0015	Derechos de uso cod.xa234	$ 1,500.00	4014863	25.0
AI-0001	Derechos de uso cod.xa742	$ 1,500.00	5207232	25.0
AI-0002	Derechos de uso cod.xa678	$ 1,500.00	9103016	25.0
AI-0003	Derechos de uso cod.xa475	$ 1,500.00	7800495	25.0
AI-0004	Derechos de uso cod.xa380	$ 1,500.00	1114119	25.0
AI-0005	Derechos de uso cod.xa259	$ 1,500.00	7876201	25.0
AI-0016	Derechos de uso cod.xa370	$ 1,500.00	4655545	25.0
AI-0017	Derechos de uso cod.xa573	$ 1,500.00	1044163	25.0
AI-0018	Derechos de uso cod.xa332	$ 1,500.00	8221950	25.0
AI-0019	Derechos de uso cod.xa471	$ 1,500.00	7059855	25.0
AI-0020	Derechos de uso cod.xa370	$ 1,500.00	4279576	25.0
AI-0021	Derechos de uso cod.xa377	$ 1,500.00	1673978	25.0
AI-0022	Derechos de uso cod.xa533	$ 1,500.00	2369428	25.0
AI-0031	Derechos de uso cod.xa110	$ 1,500.00	8423865	25.0
AI-0032	Derechos de uso cod.xa197	$ 1,500.00	9098835	25.0
AI-0033	Derechos de uso cod.xa676	$ 1,500.00	1659164	25.0
AI-0034	Derechos de uso cod.xa261	$ 1,500.00	7663396	25.0
AI-0042	Derechos de uso cod.xa434	$ 1,500.00	8849063	25.0

Filtrado de mayor a menor

Este grupo de intangibles no cumple con las políticas contables de la entidad

Existen muchos intangibles cuyas tasas de amortización son demasiado aceleradas en comparación con las políticas contables de la entidad.

Conclusión: Los valores parametrizables del sistema en cuanto a la depreciación y amortización no concuerdan con las políticas contables adoptadas, ni tampoco con los requisitos de deducibilidad establecida en la ley de impuesto sobre la renta.

VP4

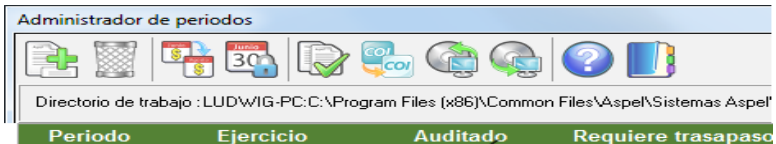
G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PVP
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: VALORES PARAMETRIZABLES

Contenido: Realice una transacción de prueba con un usuario particular y verifique si es posible registrar transacciones en un periodo cerrado y/o no habilitado.

Se solicitó acceso con el usuario jmartinez el cual corresponde al contador general, acto seguido, fue solicitado un reporte de los periodos auditados (cerrados y/o no habilitados) por el sistema, los cuales se detallan a continuación:



Periodo	Ejercicio	Auditado	Requiere trasapaso
Enero	2012	✓	
Febrero	2012	✓	
Marzo	2012	✓	
Abril	2012	✓	
Mayo	2012	✓	
Junio	2012	✓	
Julio	2012	✓	
Agosto	2012	✓	
Septiembre	2012	✓	
Octubre	2012	✓	
Noviembre	2012	✓	
Diciembre	2012	✓	
Enero	2013	✓	
Febrero	2013	✓	
Marzo	2013	✓	
Abril	2013	✓	
Mayo	2013	✓	
Junio	2013	✓	
Julio	2013	✓	
Agosto	2013	✓	
Septiembre	2013		
Octubre	2013		
Noviembre	2013		
Diciembre	2013		

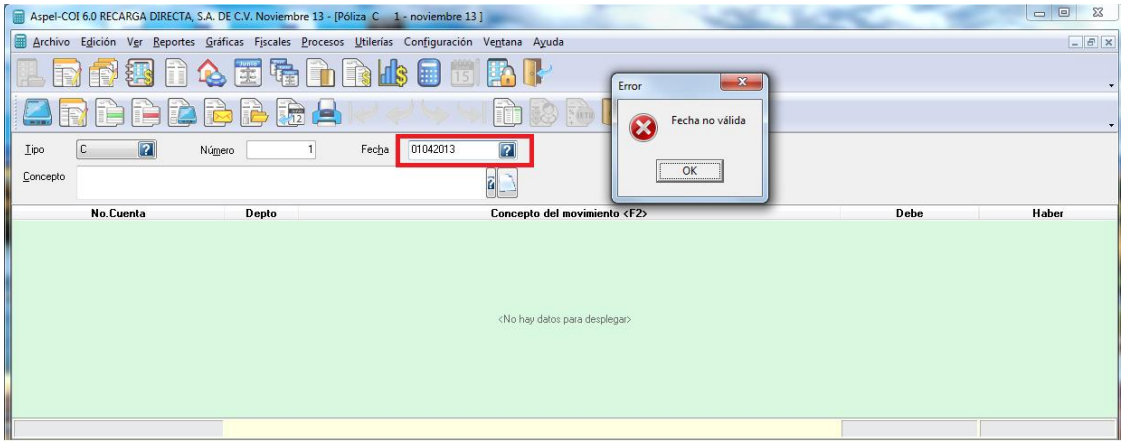
VP5

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PVP
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: VALORES PARAMETRIZABLES

Luego se intentó ingresar arbitrariamente una transacción con fecha abril de 2013, como resultado el sistema no permitió agregar pólizas de diario con el referido usuario, mostrando el siguiente mensaje de error:



Conclusión: El sistema posee una efectiva seguridad al momento en que un usuario operativo intente modificar transacciones, existe una fortaleza en el control TI.

VP5

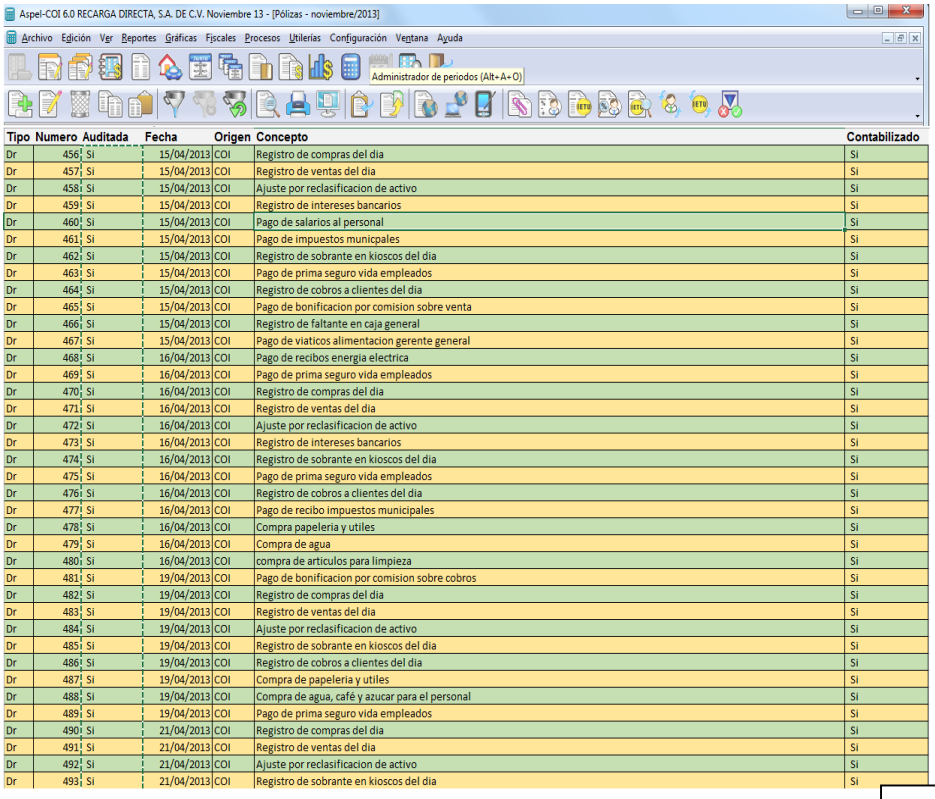
G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PVP
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: VALORES PARAMETRIZABLES

Contenido: Utilice el perfil de usuario del administrador del sistema e intente modificar transacciones en aspectos tales como, montos y fechas.

Fue solicitado el acceso al sistema con uno de los tres administradores registrados, para tal efecto se utilizó "administrador", luego con la base de datos del mes de abril 2013 se intentó modificar registros al azar, la base de datos se presenta a continuación:



Tipo	Numero	Auditada	Fecha	Origen	Concepto	Contabilizado
Dr	456	Si	15/04/2013	COI	Registro de compras del dia	Si
Dr	457	Si	15/04/2013	COI	Registro de ventas del dia	Si
Dr	458	Si	15/04/2013	COI	Ajuste por reclasificacion de activo	Si
Dr	459	Si	15/04/2013	COI	Registro de intereses bancarios	Si
Dr	460	Si	15/04/2013	COI	Pago de salarios al personal	Si
Dr	461	Si	15/04/2013	COI	Pago de impuestos municpales	Si
Dr	462	Si	15/04/2013	COI	Registro de sobrante en kioscos del dia	Si
Dr	463	Si	15/04/2013	COI	Pago de prima seguro vida empleados	Si
Dr	464	Si	15/04/2013	COI	Registro de cobros a clientes del dia	Si
Dr	465	Si	15/04/2013	COI	Pago de bonificacion por comision sobre venta	Si
Dr	466	Si	15/04/2013	COI	Registro de faltante en caja general	Si
Dr	467	Si	15/04/2013	COI	Pago de viaticos alimentacion gerente general	Si
Dr	468	Si	16/04/2013	COI	Pago de recibos energia electrica	Si
Dr	469	Si	16/04/2013	COI	Pago de prima seguro vida empleados	Si
Dr	470	Si	16/04/2013	COI	Registro de compras del dia	Si
Dr	471	Si	16/04/2013	COI	Registro de ventas del dia	Si
Dr	472	Si	16/04/2013	COI	Ajuste por reclasificacion de activo	Si
Dr	473	Si	16/04/2013	COI	Registro de intereses bancarios	Si
Dr	474	Si	16/04/2013	COI	Registro de sobrante en kioscos del dia	Si
Dr	475	Si	16/04/2013	COI	Pago de prima seguro vida empleados	Si
Dr	476	Si	16/04/2013	COI	Registro de cobros a clientes del dia	Si
Dr	477	Si	16/04/2013	COI	Pago de recibo impuestos municipales	Si
Dr	478	Si	16/04/2013	COI	Compra papeleria y utiles	Si
Dr	479	Si	16/04/2013	COI	Compra de agua	Si
Dr	480	Si	16/04/2013	COI	compra de articulos para limpieza	Si
Dr	481	Si	19/04/2013	COI	Pago de bonificacion por comision sobre cobros	Si
Dr	482	Si	19/04/2013	COI	Registro de compras del dia	Si
Dr	483	Si	19/04/2013	COI	Registro de ventas del dia	Si
Dr	484	Si	19/04/2013	COI	Ajuste por reclasificacion de activo	Si
Dr	485	Si	19/04/2013	COI	Registro de sobrante en kioscos del dia	Si
Dr	486	Si	19/04/2013	COI	Registro de cobros a clientes del dia	Si
Dr	487	Si	19/04/2013	COI	Compra de papeleria y utiles	Si
Dr	488	Si	19/04/2013	COI	Compra de agua, café y azucar para el personal	Si
Dr	489	Si	19/04/2013	COI	Pago de prima seguro vida empleados	Si
Dr	490	Si	21/04/2013	COI	Registro de compras del dia	Si
Dr	491	Si	21/04/2013	COI	Registro de ventas del dia	Si
Dr	492	Si	21/04/2013	COI	Ajuste por reclasificacion de activo	Si
Dr	493	Si	21/04/2013	COI	Registro de sobrante en kioscos del dia	Si

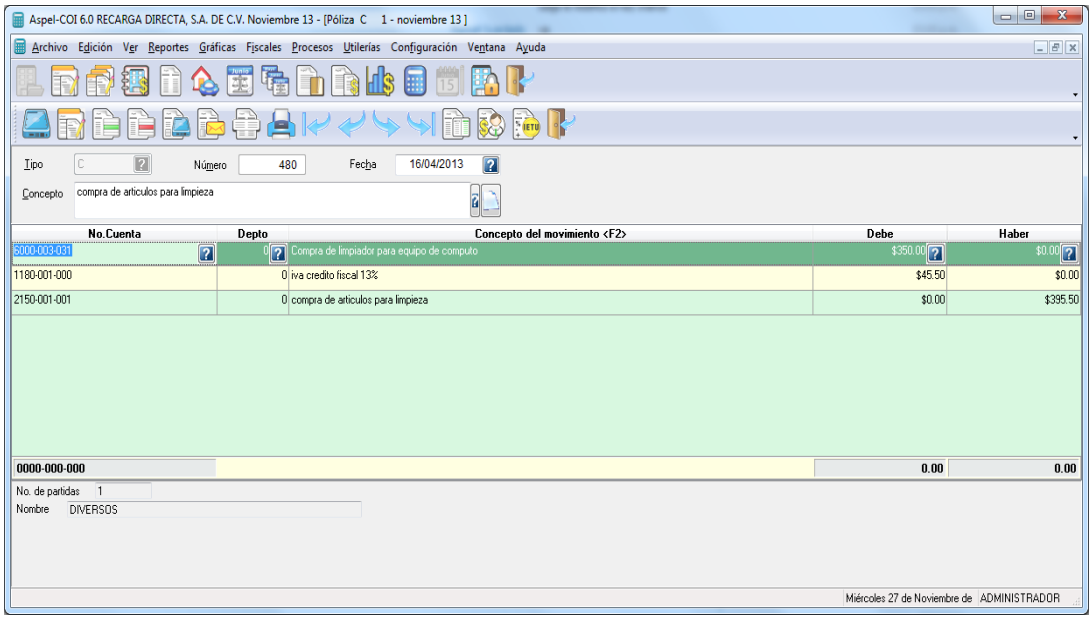
VP6

G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PVP
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: VALORES PARAMETRIZABLES

En forma aleatoria, se procedió a realizar el intento de modificación de la transacción y/o partida de diario número 480, la partida original muestra los siguientes datos:



Luego se intentó modificar lo siguiente:

a) La fecha de la partida

b) Los montos de cargos y abonos

c) Las cuentas contables

d) El concepto de la partida en forma global y en forma individual para cada cuenta

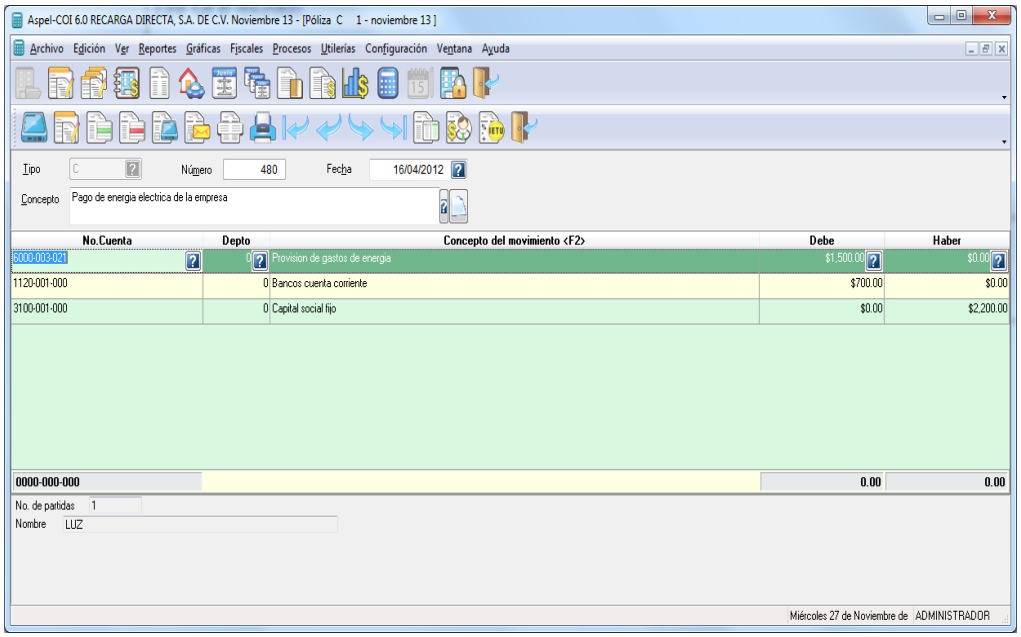
G & M, S. A. de C. V.
Auditores, Consultores y Asesores.
Avenida Sierra Nevada No. 548
Colonia Miramonte, San Salvador
A member of GM International, a group of consulting, auditing and accounting firms.

VP6

CLIENTE: RECARGA DIRECTA, S.A. DE C.V.	PERIODO	REF. P/T
SISTEMA: ASPEL COI 6.0 Y ASPEL SAE 5.0	2012	PVP
PREPARÓ: LJG	REVISÓ: OAM	

CÉDULA: VALORES PARAMETRIZABLES

Este fue el resultado:



La fecha, los montos, las cuentas y el concepto de la partida fueron modificados sin ninguna restricción.

Conclusión: Existe una grave deficiencia en el control TI sobre los accesos que poseen los administradores del sistema de ASPEL COI, cualquier *transacción* utilizada para la elaboración de los estados financieros puede ser modificada, eliminada sin el consentimiento y/o aprobación por parte de la administración de la empresa, lo cual representa un riesgo informático a considerar.

VP6