UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

"PROGRAMAS DE AUDITORÍA INTERNA PARA REALIZAR UNA EVALUACIÓN AL ÁREA DE TECNOLOGÍAS DE INFORMACIÓN BAJO EL ENFOQUE DE BUENAS PRÁCTICAS EN LAS EMPRESAS COMERCIALIZADORAS DE ELECTRODOMÉSTICOS UBICADAS EN EL ÁREA METROPOLITANA DE SAN SALVADOR"

Trabajo de investigación presentado por:

Alvarado López, Jenny Steffany

Armero Ortiz, Juan Jose

Lozano Urbina, Melissa Yamileth

Para optar al grado de:

LICENCIADO EN CONTADURÍA PÚBLICA

Noviembre de 2016

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

Rector	: Lic. José Luis Argueta Antillón
Secretaria General	: Dra. Ana Leticia Zavaleta de Amaya
Decano de la Facultad de Ciencias Económicas	: Lic. Nixon Rogelio Hernández Vázquez
Secretario de la Facultad de Ciencias Económicas	: Licda. Vilma Marisol Mejía Trujillo
Directora de la Escuela de Contaduría Pública	: Licda. María Margarita de Jesús Martínez Mendoza de Hernández
Coordinador general de Procesos de Graduación Facultad De Ciencias Económicas	: Lic. Mauricio Ernesto Magaña Menéndez
Coordinador del Seminario	: Lic. Daniel Nehemías Reyes López
Docente Director	: Licda. María Margarita de Jesús Martínez Mendoza de Hernández
Jurado Examinador	: Licda. María Margarita de Jesús Martínez Mendoza de Hernández : Lic. Carlos Ernesto Ramírez : Lic. Daniel Nehemías Reyes López

AGRADECIMIENTOS

Agradecimiento total a Dios por darme las fuerzas de seguir día a día luchando en cada una de las dificultades que pudieron surgir a lo largo del camino y por todas las personas maravillosas que me permitió conocer en este camino. A mis padres que me brindaron su apoyo incondicional para salir adelante, mi familia que estuvo apoyando cada paso de mi carrera, a mis amigos y amigas que estuvieron conmigo en momentos difíciles y amenos, a los docentes de cada una de las materias que curse los cuales me brindaron conocimiento para poder aplicarlo en el diario vivir y a esas personas que me apoyaron en alguna etapa de mi formación profesional y personal.

Jenny Steffany Alvarado López.

Gracias a Dios por haberme permitido culminar una fase importante en mi vida, por otorgarme la sabiduría necesaria para afrontar cada obstáculo y lograr superarlo, por ser la guía que necesite cuando no encontraba la salida en muchas situaciones, por todo eso y más, gracias. Gracias a mi familia ya que sin su incondicional apoyo no hubiera logrado lo que hasta hoy he hecho, por permitirme seguir mis sueños no importando la dificultad de estos, por dejar desarrollarme como persona y como profesional, por demostrarme su amor en los momentos que más lo necesite, por todo eso y más, gracias. Gracias a cada uno de los profesionales docentes que contribuyeron con mi formación académica y aún más a los que aportaron con sus consejos para poder afrontar mi vida de manera adecuada, por verme no solo como un alumno, sino como un amigo, por su confianza y por su tiempo dedicado hacia mi persona, por todo eso y más, gracias. Gracias a todas las personas que de una u otra manera me apoyaron, confiaron y comparten este triunfo conmigo, GRACIAS.

Juan Jose Armero Ortiz.

Primeramente a Dios y la Virgen María por darme sabiduría, por guiarme a lo largo de este camino, darme fortaleza y perseverancia para seguir adelante y llegar a esta etapa de culminación de la carrera universitaria. A mis padres y mi familia que han contribuido a mi formación profesional, así como también formación personal, gracias por estar de manera incondicional dándome su apoyo, ayuda, paciencia y ánimos para seguir luchando por alcanzar mis objetivos. A mis amigos que han sido parte esencial para lograr esto, que siempre han estado allí para darme ánimos de seguir adelante y ayudándome con sus palabras de aliento. A mis compañeros de tesis por esa amistad que formamos dentro de este proceso, por su disposición, aporte y colaboración para salir adelante. A mis catedráticos, asesores, profesores, maestros, directores que me han formado profesionalmente para llegar a cumplir este objetivo y dejar una huella en mi crecimiento personal. A todas personas que conocí a lo largo de mi formación profesional que contribuyeron con su granito de arena para alcanzar este logro.

Melissa Yamileth Lozano Urbina.

ÍNDICE

ÍNDICE DE TABLAS, FIGURAS Y ANEXOS.

RESUMEN EJECUTIVO

La actividad de auditoría interna es una actividad independiente y objetiva de supervisión y consultoría diseñada para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno. El alcance que esta posee dentro de las empresas es amplio ya que puede incluir diferentes enfoques, dentro de ella se aplican las auditorías internas hacia las tecnologías de información para evaluar las áreas de software, hardware, seguridad física, seguridad lógica, procesamiento electrónico de datos y recursos humanos.

La evaluación a las tecnologías de información es importante para las empresas debido a que por medio de ellas se llevan a cabo los procesos críticos de la entidad, así como también el manejo de la información significativa, al evaluar dicha área contribuye a agregarle valor a la gestión como lo sugiere la NIEPAI, a los procesos que se llevan a cabo por medio de las tecnologías de información.

Para la elaboración de la investigación la fuente principal que se tomó como base fueron los auditores internos y sus colaboradores, la recolección de la información se llevó a cabo por medio de cuestionario de preguntas cerradas y de selección múltiple para conocer la situación actual de las empresas comercializadoras de electrodomésticos respecto al área de tecnologías de información, posteriormente se procedió a realizar el diagnóstico de la información que se recolectó por medio de cruce de variables dependiente e independiente, hasta llegar a la identificación de aspectos importantes a evaluar respecto al área de tecnologías de información.

Dentro de los aspectos a evaluar luego de los resultados obtenidos es que el perfil del recurso humano cuente con los aspectos necesarios para llevar a cabo las actividades de auditoría interna, así como también el nivel de capacitación que este posee ya sea en el área de tecnologías de información como buenas prácticas y si aplican estos conocimientos al momento de llevar a cabo las auditorías y evaluar si el personal cumple con lineamientos y procedimientos en el caso de uso, cuidado y mantenimiento del activo tecnológico.

INTRODUCCIÓN

Actualmente la práctica de auditoría interna conlleva que el auditor permanezca en constante actualización por los diferentes avances que se dan entorno a todas las áreas de negocio que se evalúan, los cambios en leyes y normativas aplicables que rigen las actividades de las entidades, avances tecnológicos, así como marcos de referencia utilizados para la ejecución del trabajo de auditoría.

De acuerdo a lo anterior y observando la necesidad que poseen los auditores internos por falta de una guía para la evaluación al departamento de tecnologías de información de empresas dedicadas a la venta de electrodomésticos, se diseñó un plan de auditoría interna el cual está basado en normativa técnica conocida en nuestro medio como “buenas prácticas” ya que son marcos normativos que no son de obligatorio cumplimiento en el país pero su aplicación conlleva a generar valor extra a los procesos efectuados en la entidad.

Con base a lo descrito en el párrafo anterior y con la finalidad de brindar una herramienta a auditores internos en su trabajo, se desarrolla el presente documento, estructurado en cinco capítulos.

Capítulo I, se desarrolla la situación problemática la cual define el origen del problema a investigar, el enunciado del problema, la justificación de la investigación a realizar, además contiene los objetivos trazados para la realización de la investigación, así como también las limitantes de la investigación, incluye también la hipótesis de la investigación y por último la forma en la que se llevara a cabo el diagnóstico de la investigación.

Capítulo II, Se detalla la situación actual del problema de investigación, así como una serie de principales definiciones que enmarcan la investigación, además este capítulo incluye legislación y normativa técnica aplicable al tema a desarrollar

Capítulo III, desarrolla la metodología a utilizar, el enfoque y el tipo de investigación que se realizará, la delimitación geográfica de la investigación así como también la delimitación temporal, se presenta además los sujetos y el objeto de investigación, así como también se detalla las técnicas y los instrumentos que servirán de ayuda en la recolección de información para la realización de la investigación, además se presenta el procesamiento, el análisis y la interpretación de los datos procesados, para finalizar se desarrolla el diagnóstico de las diferentes áreas que fueron sujetas a investigación.

Capítulo IV, desarrolla la propuesta del plan de auditoría interna, estableciendo inicialmente un estudio para determinar el conocimiento preliminar que se tiene de la entidad detallando su estructura organizativa, las áreas de negocio, los procesos importantes que se efectúan en la entidad, presentado luego la legislación aplicable a las entidades comercializadores de electrodomésticos, posteriormente se desarrolla el plan anual de auditoría interna, se presenta un ejemplo de memorándum de planeación, evaluación de control interno a procedimientos de tecnologías de información a través de cuestionarios dando como resultado una matriz de riesgo, finalizando con los programas de auditoría interna para realizar una evaluación al área de tecnologías de información bajo el enfoque de buenas prácticas en las empresas comercializadoras de electrodomésticos.

1. CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1 SITUACIÓN PROBLEMÁTICA

Con el inicio del siglo XXI y el auge de nuevas tecnologías que simplifican los procedimientos, las empresas se vieron en la necesidad de apertura departamentos de informática, además del surgimiento de normativas técnicas como COBIT 5 y las normas de calidad ISO 27001 e ISO 27002 que son aplicables a esta área, las cuales sugieren lineamientos para el desarrollo de los procesos en el área de tecnologías de la información y que a pesar que no son de obligatorio cumplimiento se pueden implementar como "buenas prácticas" para evitar riesgos que afecten en el futuro a la entidad.

Los encargados del departamento de informática están en la obligación de velar por el cumplimiento de los siguientes principios: la satisfacción de las necesidades de las partes relacionadas, cubrir la compañía de forma integral, aplicar un solo marco integrado, habilitar un enfoque holístico y separar el gobierno de la administración, que se establecen en la normativa técnica COBIT 5 respecto al área de tecnologías de información, debido a esto el objetivo a cumplir es realizar un control adecuado sobre el uso y mantenimiento de las herramientas informáticas en las entidades comercializadoras de electrodomésticos; por el tipo de información que se maneja y haciendo uso de una herramienta como lo es la tecnología, debe realizar una evaluación que permita el cuidado y control de los datos utilizados, ya que la pérdida de información puede significar costos significativos para las empresas, así como también para el uso y protección de los equipos en los que está respaldada dicha información.

Debido a que actualmente no se cuenta con un marco legal que sea dirigido específicamente al área de informática, y la poca relevancia en la aplicación de procedimientos para la evaluación de la unidad de tecnologías de información, es sumamente importante que se realicen evaluaciones a la normativa técnica bajo el enfoque de "buenas prácticas", ya que el área informática dentro de las empresas es de mucha importancia y está en constante crecimiento

Las deficiencias que se puede generar como resultado de no realizar una evaluación a los lineamientos que establece la normativa COBIT 5, están basadas en amenazas que afectan el uso y cuidado del hardware, software, seguridad lógica, seguridad física, redes, y telecomunicaciones, ya que de incumplir en el cuidado de estos se podría incurrir en la perdida de información de uso confidencial, la cual puede ser usada con fines inadecuados, así como también el cuidado de los equipos informáticos que resguardan dicha información.

Por esta razón es que los auditores internos deben crear procedimientos que encaminen a realizar de manera efectiva la evaluación del área de tecnologías de información de las empresas, ya que se debe evaluar aspectos desde la seguridad física de los elementos hasta los procedimientos lógicos que se efectúen, sobre todo por el tipo de información que se pueda manejar en las instituciones, en este caso para las empresas que se dedican a la comercialización de electrodomésticos.

Una evaluación a la normativa técnica aplicable al departamento de tecnologías de la información bajo el enfoque de buenas prácticas es fundamental, para el alcance de los

objetivos y las estrategias corporativas que poseen las empresas comercializadoras de electrodomésticos.

La trascendencia de realizar una evaluación de la normativa técnica COBIT 5 e ISO 27001 y 27002 aplicable al área de tecnologías de la información es realizar una auditoría que cubra riesgos informáticos que pueden afectar a la empresa, además de dar respuesta y realizar acciones para minimizar dichos riesgos, con el fin de llegar a un riesgo aceptable o tolerado por la entidad, así mismo la sugerencia de políticas y procedimientos que se puedan establecer e implantar para ayudar a asegurar que las respuestas al riesgo se llevan a cabo eficazmente.

Existe una diversidad de dificultades que pueden afectar a la empresa de las cuales el departamento de informática es el encargado de identificar y solventar, entre las cuales se pueden observar la falta de baterías para computadoras (UPS) o en mal estado, falta de mantenimiento preventivo para los equipos, programas informáticos sin licencia original, todo lo anterior perjudica el desempeño de los equipos y el resguardo de la información, ya que existe un lineamiento que regula la obligación de resguardar el equipo informático tanto en seguridad física como en seguridad lógica, en el caso de no cumplir con esto tendría como consecuencia la perdida de información que mucha de ella puede ser de uso confidencial.

Al no realizar una auditoría con enfoque de buenas prácticas basado en la normativa técnica COBIT 5 ISO 27001 y 27002, a las empresas comercializadoras de electrodomésticos, se podrían ver afectados los intereses tanto económicos como los requerimientos de personas que mantengan interés sobre las entidades de este tipo ya sea como los proveedores, instituciones

bancarias e inversionistas, debido a que este sector depende en gran medida de sistemas automatizados para sus procesos de inventarios, gestión de cobros, manejo de su cartera de clientes e inclusive manejo de ventas en línea, debe de evaluarse el sistema de tal manera que cumpla con las necesidades para el manejo de esa información, así como la protección del mismo de amenazas como virus, intrusiones no deseadas, perdida de información de carácter confidencial, modificaciones a los registros sin autorización, colapsos del sistema por la cantidad de operaciones que se realicen dentro de él, entre otras.

Debido al incremento de dispositivos móviles para el uso de las actividades diarias de estas entidades como lo son el uso de post, equipos informáticos portátiles, memorias USB, entre otros, su uso debe estar regulado bajo procedimientos de normativa aplicable, ya que el cuidado de los equipos debe realizarse en las áreas determinadas como seguridad física, seguridad lógica, redes y comunicaciones, hardware y software, de manera que es más susceptible a uso inadecuado, esto generaría que el equipo no tuviera las medidas necesarias para su cuidado dentro de esto, se ve afectada la perdida de información de carácter importante para la empresa, cabe mencionar que la protección de dicha información debe estar respaldada en back up y estos deben estar resguardadas como las normas de buenas prácticas lo establecen.

1.2 ENUNCIADO DEL PROBLEMA

En los últimos años los auditores se han enfocado fundamentalmente en trabajos del área financiera y de cumplimiento fiscal, para satisfacer las necesidades de las entidades a las cuales les prestan sus servicios y para terceras personas las cuales solicitan información sobre dichas

organizaciones, enfocándose principalmente en áreas más operativas o en auditorías de gestión a los diversos departamentos, debido a lo anterior los auditores no cuentan con programas especializados basados en COBIT 5 y las normas de calidad ISO 27001 y 27002 que permitan la evaluación a los procesos realizados en el área de tecnologías de información, a pesar de que esta unidad proporciona información de suma importancia para el funcionamiento de las empresas comercializadoras de electrodomésticos.

Es por ello que se orienta el estudio en proponer programas que orienten al auditor interno en la evaluación al departamento de informática, mediante la aplicación de buenas prácticas que sugiere la NIEPAI.

¿En qué medida afecta la falta de procedimientos basado en COBIT 5 e ISO 27001 Y 27002, para realizar una evaluación de auditoría interna bajo el enfoque de buenas prácticas que sugiere las Normas Internacionales para el Ejercicio Profesional de Auditoría Interna, en el logro de los objetivos estratégicos del departamento de tecnologías de información en las empresas dedicadas a la venta de electrodomésticos en el área metropolitana de San Salvador?

1.3 JUSTIFICACIÓN DE LA INVESTIGACIÓN

Con el surgimiento de nuevas tecnologías y la aplicación de nuevos procedimientos que ayuden al manejo de la información, así como la poca relevancia que posee el tema en investigaciones anteriores, se determinó que actualmente no existen programas con aspectos técnicos que estén basado en los lineamientos de COBIT 5 e ISO27001 y 27002, que contribuyan

para que el auditor interno pueda efectuar una evaluación al departamento de tecnologías de información de las empresas dedicadas a la comercialización de electrodomésticos haciendo uso de los consejos de buenas prácticas de las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna (NIEPAI).

Un documento que incluya programas para el desarrollo de una evaluación por parte de auditoría interna es novedoso, ya que plantea lineamientos para el diagnóstico de los procedimientos que incluya desde el cuidado que debe tenerse en seguridad física y lógicas hasta el software, hardware y redes telecomunicaciones en el departamento de tecnologías de información.

En investigaciones realizadas anteriormente estaban basados en el diseño de sistemas informáticos en diferentes sectores empresariales, sin embargo esta investigación está fundamentada en la realización de programas de auditoría al departamento de informática bajo el enfoque de buenas prácticas.

1.4 OBJETIVOS DE LA INVESTIGACIÓN

1.4.1 GENERAL

Elaborar plan de auditoría interna que sean utilizados como herramienta por las unidades de Auditoría Interna bajo el enfoque de buenas prácticas que sugiere las Normas Internacionales para el Ejercicio Profesional de Auditoría Interna, para la realización de evaluaciones al

cumplimiento de la normativa técnica aplicable en el área de Tecnologías de Información, en las empresas del sector comercio dedicadas a la venta de electrodomésticos.

1.4.2 ESPECÍFICOS

- Recopilar información bibliográfica referente al tema de investigación.
- Realizar una investigación de campo que permita identificar la situación actual de la profesión de auditoría interna referente a la aplicación de procedimientos con enfoque en buenas prácticas para el área de tecnologías de información.
- Proponer un plan de auditoría interna que contenga todos los aspectos relativos a la aplicación de buenas prácticas en el área de tecnologías de información.
- Concluir y proponer.

1.5 HIPÓTESIS DE INVESTIGACIÓN.

Elaboración e implementación de programas para la realización de una evaluación al departamento de tecnologías de información por parte de auditoría interna bajo el enfoque de buenas prácticas, que contribuyan al alcance de los objetivos estratégicos de la entidad y al cumplimiento de la normativa técnica en el manejo, uso y cuidado del sistema informático y sus componentes.

1.6 LIMITACIONES DE LA INVESTIGACIÓN

La investigación se encontró limitada por las siguientes causas:

1.6.1 Características de la muestra

Dentro de la población que se estudió existen diversos estratos, como lo son auditores internos, ingenieros, programadores y personal de mantenimientos de sistemas; esto no permitió obtener una muestra homogénea debido a que no todos poseen los mismos conocimientos.

1.6.2 Sesgo del sujeto.

Las respuestas obtenidas al realizar entrevistas y pasar cuestionarios dependieron del grado de conocimiento que poseen los sujetos de estudio acerca de las normas COBIT 5 e ISO 27001 y 27002.

1.6.3 Disposición por parte de los empleados

La disposición de los empleados en brindar información necesaria para la realización de la investigación o disposición de tiempo por parte de ellos por sus ocupaciones laborales.

1.6.4 Acceso a los departamentos informáticos por parte de las empresas estudiadas

Acceso a los departamentos por la inseguridad que pueda causar dentro de las empresas el observar procesos críticos dentro de ellas.

2. CAPÍTULO II: MARCO TÉORICO.

2.1 SITUACIÓN ACTUAL DE LA INVESTIGACIÓN

La auditoría interna ha tenido la necesidad de evolucionar para adecuarse a los constantes cambios que se han dado en las entidades para lograr un equilibrio entre las expectativas que tiene el comité de auditoría interna y la alta gerencia en el alcance de los objetivos estratégicos planteados; así como definir tres líneas de defensa para identificar los riesgos, esto como parte de una nueva tendencia en el área de auditoría interna la cual desarrolla lineamientos a seguir para mitigar los riesgos, en la primera línea la gerencia gestiona los riesgos, también son los responsables de implementar acciones correctivas para abordar el proceso y las deficiencias de control, en la segunda línea la contraloría además de los encargados de la gestión de riesgos, de las funciones de cumplimiento, de seguridad, de calidad facilitan y supervisan la implementación de prácticas de gestión de riesgos que ha propuesto la gerencia , en la tercera línea de defensa se encuentra la auditoría interna la cual basada en un enfoque de riesgos proporciona monitoreo y seguimiento sobre la gestión del gobierno corporativo, la gestión de riesgos, el control interno y además verifica el funcionamiento de la línea uno y dos de defensa.

En la medida que los ejecutivos de las compañías quieran estar seguros de dar soluciones a problemas que se generan en la entidad, estos tendrán que decidir quiénes dentro de sus organizaciones van a tener su confianza para ayudarles a mitigar efectivamente los riesgos que cada área de la empresa este presentando, cabe destacar que, si los departamentos de Auditoría Interna quieran ocupar este espacio, que realmente parece diseñado para ellos, van a tener que

afrontar una gran transformación para poder llegar a convertirse en “asesores de confianza” del gobierno corporativo de las compañías.

En primer lugar, hay que considerar la naturaleza del enorme reto que tiene ante sí el gobierno corporativo. Ha llegado el momento en el que, desde su posición de liderazgo, deberían ayudar a poner fin a la polémica estéril derivada de la teoría del “mal necesario”, según la cual los auditores internos deben existir por razones diversas, pero ninguna relacionada con el hecho de que su trabajo resuelve problemas de relevancia similar a los que resuelven los especialistas en finanzas, los ingenieros o los analistas de riesgos.

Los auditores internos se perfilan como un “bien imprescindible, irrenunciable e insustituible” para los altos ejecutivos, pues aquéllos están en una posición inmejorable para ofrecer información veraz y objetiva de en qué medida el día a día de las empresas está siendo gestionadas en todas sus áreas.

En segundo lugar, para los auditores internos el reto que se plantea es de grandes dimensiones, probablemente nadie pueda ayudar más, en esta nueva era, a los auditores internos que ellos mismos, ya que a parte del rol que ya desempeñaban, estos deben realizar una gestión más ética y una mayor contribución al progreso social en el sector donde las empresas desarrollan su actividad.

En todo caso, la proyección de la competencia profesional de los auditores internos hacia medidas más elevadas se verá facilitada por el desarrollo individual de los siguientes atributos:

1) Profesionalización: hoy para un auditor interno, la profesionalidad no debería ser, otra cosa que mostrar siempre “la razón del sentido común”.

2) Especialización: hoy no es posible pensar en auditores internos generalistas que aborden tangencialmente los temas que analizan, a veces utilizando como palanca la literalidad de normas, reglamentos o regulaciones que puede no hayan sido objeto de una reflexión profunda y objetiva.

3) Capacitación gerencial: hoy un auditor interno debe disponer de habilidades relacionales más desarrolladas que las de la mayoría de los demás profesionales de la empresa. El trabajo del auditor interno tiene mucho de persuadir, de inducir, de convencer, de incitar, de impulsar el comportamiento de otros para que adopten decisiones en una determinada dirección.

4) Formación continua: hoy la velocidad con la que se desarrollan los procesos de innovación técnica, tecnológica y de negocio exigen al auditor interno disponer de un plan de formación continua que le permita no perder el tren del conocimiento especializado.

5) Tecnologías de la información: hoy es una necesidad para los auditores internos disponer de conocimientos sólidos en el tratamiento masivo de datos. Probablemente se

ha iniciado un camino en el que las tradicionales pruebas muéstrales van a dejar paso a los análisis censales, impulsados por las posibilidades que ofrecen las tecnologías de la información.

6) Excelencia: hoy los auditores internos deben ser conscientes de que su rol, el rol que pueden jugar en esta nueva era, solo es posible desarrollarlo ofreciendo niveles de competencia profesional compatibles con la excelencia.

Las compañías se enfrentan en la actualidad a una variedad de nuevos desafíos en su intento de maximizar su valor. La globalización, los e-business, las nuevas sociedades organizacionales y la velocidad cada vez mayor de la actividad de los negocios están cambiando rápidamente y expandiendo los riesgos a los que se enfrenta la organización.

En este contexto, para la función de Auditoría Interna el uso de nuevas tecnologías se convierte en un factor clave. Auditoría Interna debe evolucionar hacia modelos QERM (gestión de riesgos empresariales cuantitativos), que aporten análisis y selección de metodologías de cuantificación. Modelos de auditoría continua donde se definan indicadores KRIs (indicadores de riesgos clave) y controles, donde se pueda definir y cuantificar el apetito al riesgo de las compañías, los umbrales y los límites de tolerancia.

El uso de las tecnologías aporta a la función una visión dinámica y activa que permite responder consistente, eficiente y rápidamente a los riesgos que surjan y a los requerimientos regulatorios cambiantes.

El departamento de Auditoría Interna, como responsable de la evaluación del entorno de control interno, debe mantener el paso de las nuevas tecnologías. Estos cambios no suponen únicamente la adaptación de nuevas herramientas para la realización de su trabajo tradicional, sino que suponen un cambio de mentalidad en cuanto al enfoque del trabajo realizado por los auditores internos.

Podemos plantear la relación del auditor interno con las nuevas tecnologías en tres niveles o planos diferentes.

- En primer lugar, está la forma en que la tecnología está presente actualmente en todas las transacciones de una empresa. Esto supone en muchas ocasiones un cambio en la planificación de las pruebas de auditoría tradicionales, así como en su propia definición.

- En segundo lugar, las nuevas tecnologías ofrecen al auditor un amplio abanico de posibilidades para profundizar en su trabajo, aumentar el rendimiento del mismo y permitir un mayor control sobre cualquier tipo de operación.

- Por último, el desarrollo de las tecnologías supone un nuevo campo que debe ser objeto de supervisión por parte del auditor, surgiendo una Auditoría Interna especializada en los sistemas de información, con sus propias características, incluyendo legislación específica de obligado cumplimiento.

  (Instituto de Auditores Internos de España, 2015)

2.2 PRINCIPALES DEFINICIONES

Auditoría de cumplimiento: Es la aprobación o examen de las operaciones financieras, administrativas, económicas y de otra índole de una entidad para establecer que se ha realizado conforme a las normas legales, reglamentarias, estatutarias y de procedimiento que le son aplicables. Esta auditoría se practica mediante la revisión de los documentos que soportan legal, técnica, financiera y contablemente las operaciones para determinar si los procedimientos utilizados y las medidas de control interna están de acuerdo con las normas que le son aplicables, si dichos procedimientos están operando de manera efectiva y si son adecuados para el logro de los objetivos de la entidad.

(Preparatorio Auditoria, pág. s/n)

Hardware: Es la parte física del ordenador o sistema informático, está formado por los componentes eléctricos, electrónicos, electromecánicos, tales como: circuitos de cables y circuitos de luz, placas, utensilios, cadenas y cualquier otro material en estado físico que sea necesario para hacer que el equipo funcione. (Significados, pág. s/n)

Modem: Es un dispositivo que “transforma” la señal que envía la computadora en una señal que puede ser “transmisible” por el vínculo.

(Cortagerena, et.al. 2001, pág. 66)

Sistema operativo: Es el software de más bajo nivel, indica y supervisa las operaciones de la CPU, sus componentes pueden agruparse así: Programas de carga inicial, programas de control. (Cortagerena, 2001, pág. 40)

Software: Es el conjunto de instrucciones que controlan el funcionamiento del sistema de computación. Es decir, el software le "da vida" al hardware, le da una razón de ser, una finalidad. (Cortagerena, et.al. 2001, pág. 39)

Tecnologías de Información y comunicación: Son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro, abarcan un abanico de soluciones muy amplio. Incluye las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro o procesar información para poder calcular resultados y elaborar informes.
(Servicios TIC, pág. s/n)

2.3 LEGISLACIÓN APLICABLE

2.3.1 Regulaciones Específicas

- **Ley de firma electrónica**

Dentro de las legislaciones especificas aplicables a las empresas comercializadoras de electrodomésticos es la Ley de Firma electrónica que contempla lo relacionado a la validez que posee este mecanismo siempre y cuando este certificada, así como también la seguridad que

tienen los archivos que viajan por medios magnéticos, sobre todo si son datos personales de los clientes, en este caso no puede revelarse información que pueda afectar la imagen de los mismos; entre los aspectos que la ley menciona esta uso de medios electrónicos para el almacenamiento de datos y para ello se deben acatar las medidas de seguridad necesaria ya sea técnica, física u organizativa.

El uso de la firma electrónica debe cumplir con ciertos efectos como es vincular un mensaje de datos con su titular de manera exclusiva, así como también permita la verificación inequívoca de la autoría e identidad del signatario y asegurar que los datos de la firma estén bajo control exclusivo del signatario.

- **Ley de impuesto a las operaciones financieras**

Debido a que este tipo de empresas poseen un volumen elevado de transacciones electrónicas con sus proveedores y esto se encuentra enumerado en los hechos generadores del impuesto a las transacciones financieras, que están reguladas por medio de la Ley de impuesto a las operaciones financieras, la cual aplica un impuesto especial a las transferencias electrónicas que se realicen en el territorio nacional y sean en la moneda de legal circulación en el mismo.

Este impuesto se aplicará a las operaciones financieras en un 0.25% sobre el monto de la transacción ya sea depósitos, pagos o retiros en efectivo.

- **Ley especial contra los delitos informáticos y conexos**

Es de suma importancia la aplicación de esta ley en las empresas comercializadoras de electrodomésticos ya que este tipo de entidades proporcionan una gran cantidad de créditos a sus

clientes y es por esta razón que la información debe estar debidamente protegida de delitos informáticos, ya que al no estar protegida se atenta contra la confidencialidad, integridad, seguridad y disponibilidad de los datos en general.

La ley tiene por objeto la protección de la información de conductas delictivas cometidas por medio de las Tecnologías de Información y la Comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes.

- **Ley de regulación de los servicios de información sobre el historial de crédito de las personas**

Uso y tratamiento que se le debe dar a la información que se obtiene de los clientes.

2.3.2 Regulaciones Generales

- **Código de Comercio**

El Código de Comercio es de suma importancia ya que las disposiciones aquí establecidas rigen a los comerciantes, tanto personas naturales como sociedades, además de todos los actos de comercios que estos efectúan y las cosas mercantiles.

- **Código Tributario y su reglamento**

Utilización de formularios u otros medios tecnológicos para declarar, normas administrativas sobre emisión de los documentos y emisión de tiquetes en sustitución de facturas por medio de máquinas registradoras u otros sistemas computarizados

- **Ley de Impuesto sobre la Renta**

Tipos de ingresos que son gravados y los cuales deben cancelar impuestos, así como los gastos que poseen las empresas sean deducibles del impuesto sobre la renta.

- **Ley de impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios**

La ley de IVA como comúnmente es conocida, es la que rige el impuesto a la transferencia de bienes que en nuestro país es el 13%, las empresas investigadas por ser su giro la venta de electrodomésticos es importante la aplicación de la ley.

Estas entidades que están bajo esta ley están en la obligación de realizar las diferentes disposiciones que se exigen como la elaboración de libros por ventas a contribuyentes, libros por ventas a consumidores finales y libros de compras, la presentación de declaraciones mensualmente, entre otros.

- **Ley Contra el Lavado de Dinero y Activos**

Las entidades dentro de las obligaciones que posee es someterse a las leyes y reglamentos que así lo estipulen las autoridades de la región dentro de ellas está la aplicación de la Ley contra el lavado de dinero y activos que dentro de ella establece los obligados a aplicar esta ley y como sociedad está obligado a realizar sus actividades comerciales de manera licita y transparente, sin administraciones fraudulentas o enriquecimiento ilícito, o en su caso evasión de impuesto o estafa, ya que al cometer alguna de estas faltas se incurre en infracciones penales en su caso.

Para que las entidades estén al día con la aplicación de esta ley y para realizar sus transacciones financieras, debe poseer la certificación de la Unidad de Investigación Financiera que cumple con los requisitos establecidos por la ley antes mencionada, como por ejemplo llevar un control indicado de forma automatizada para identificación de sus clientes y usuarios, de acuerdo a los formatos establecidos por la Unidad de Investigación Financiera, que contienen por ejemplo nombre completo de los clientes, fecha y hora de la transacción entre otros, todo esto con el fin de llevar sus operaciones de manera legal.

2.4 NORMATIVA TÉCNICA APLICABLE

Debido a que las tecnologías de información actualmente forman una parte importante dentro de las prácticas diarias se encuentran normativas aplicables a dicha área que ayuden al uso, manejo y cuidado de las mismas, dentro de estas normativas aplicables esta Control Objectives for Informations and Related Technology 5 (COBIT por sus siglas en Ingles), u Objetivos de Control para la Información y Tecnología Relacionada, por su traducción al español, ya que ayuda a que las empresas creen un valor óptimo de la tecnología de información que logre obtener un equilibrio entre los beneficios, los riesgos y recursos que posee la entidad.

Ya que la seguridad de la información puede generar riesgos dentro de la gestión de la empresa la normativa de calidad aplicable al área de tecnologías de información es International Organization for Standardization (ISO por sus siglas en siglas), u Organización Internacional de Normalización por su traducción al español en las ISO 27001 e ISO 27002; la primera de ellas aspectos sobre la ciberseguridad, esto contribuye dentro de la auditoría interna a identificar los

riesgos y a la vez establecer los controles para disminuir los riesgos, dando esto seguridad a las partes interesadas con respecto a la protección de los datos que se manejan en la entidad, logrando alcanzar los objetivos estratégicos planteados por la empresa; la normativa ISO27002 hace referencia a las políticas de seguridad de información dentro de las instituciones tanto en seguridad física y de su entorno como seguridad lógica, que comprende el uso, cuidado y mantenimiento del activo tecnológico, así también la aplicación para la gestión de incidentes que se puedan ocasionar a las tecnologías de información por ejemplo intrusiones no deseadas, vulnerabilidades técnicas, software maliciosos, entre otros.

Para llevar a cabo una auditoría se necesita conocer los riesgos por los que se ve afectada la entidad, para determinar dichos riesgos se utiliza la normativa aplicable que nos muestra una guía que ayuda a definir en qué medida pueden afectar a la empresa en caso de ocurrencia, esta misma proporciona las posibles soluciones a dichos riesgos, Committee of Sponsoring Organizations of the Treadway Commission (COSO por sus siglas en inglés) o Comité de Organizaciones Patrocinadoras por su traducción al español, COSO ENTERPRISE RISK MANAGEMENT (ERM por sus siglas en ingles), Gestión de Riesgo Empresarial por su traducción al español, es utilizado dentro de la auditoría interna, porque contribuye a la identificación de todos los aspectos que deben estar presentes para administrar el riesgo, y esto trae beneficios a la entidad a razón de que ve incrementada la capacidad de asumir de manera adecuada los riesgos y de esa manera agregar valor como lo establece en la definición de la auditoría interna.

Los auditores deben tener conocimientos sobre riesgos y controles claves con respecto a las tecnologías de información, basados en normativa aplicable a buenas prácticas para llevar a cabo

auditorías internas en las empresas las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna (NIEPAI) establecen una serie de lineamientos aplicables, dentro de los cuales establece tanto el uso de tecnologías de información que permitan desempeñar el trabajo asignado, como la evaluación de si el gobierno de tecnología de la información de la organización apoya las estrategias y objetivos de la organización; las obligaciones de los auditores al realizar una auditoría es dejar constancia de cada uno de los procesos que se lleven a cabo, incluyendo alcance, objetivos, tiempo y asignación de recursos, todo esto como las buenas prácticas establecidas.

1210- Aptitudes

1210-.A3 Los auditores deben tener conocimientos suficientes de los riesgo y controles clave en tecnología de la información y de las técnicas de auditoría interna disponibles basadas en tecnología que le permitan desempeñar el trabajo asignado.

1220-Cuidado Profesional

1220-A2 Al ejercer el debido cuidado profesional el auditor interno debe considerar la utilización de auditoría basada en tecnología y otras técnicas de análisis de datos.

2110- Gobierno

2110-A2 La actividad de auditoría interna debe evaluar si el gobierno de tecnología de la información de la organización apoya las estrategias y objetivos de la organización.

2010-El director ejecutivo de auditoría debe establecer un plan basado en los riesgos, a fin de determinar las prioridades de la actividad de auditoría interna. Dichos planes deberán ser consistentes con las metas de la organización.

2200- Los auditores internos deben elaborar y documentar un plan para cada trabajo, que incluya su alcance, objetivos, tiempo y asignación de recursos.

2400-Comunicación de resultados. Los auditores internos deben comunicar los resultados de los trabajos.

3. CAPÍTULO III: METODOLOGÍA DE LA INVESTIGACIÓN.

3.1 ENFOQUE Y TIPO DE INVESTIGACIÓN

La investigación fue realizada bajo el enfoque cuantitativo, se utilizaron datos estadísticos asignado valores numéricos para crear probables relaciones de las variables establecidas luego de realizar un proceso riguroso con el fin de dar respuesta a los problemas a través de un proceso sistemático.

Asimismo se desarrolló la investigación bajo el método hipotético deductivo que lleva la indagación encaminada de una actividad realizada de manera general hasta llegar a lo específico, partiendo desde investigar la auditoría de forma general, hasta llegar a la aplicación de la normativa técnica al área de informática de las empresas dedicadas a la comercialización de electrodomésticos en El Salvador. Este método permitió for*m*ar una hipótesis y deducción por medio de la observación de la realidad, para ello se hizo uso de técnicas e instrumentos que ayudaron a la recolección de la información referente al departamento de informática, de la mano de la unidad de auditoría interna, así como también el personal clave del departamento de informática, esto contribuyo a realizar un análisis adecuado para desarrollar la hipótesis planteada.

3.2 DELIMITACIÓN ESPACIAL Y TEMPORAL.

3.2.1 Espacial o geográfica

La investigación se desarrolló en las empresas dedicadas a la comercialización de productos electrodomésticos, que poseen dentro de su organización unidad de auditoría interna, ubicadas en el área metropolitana de San Salvador, lo anterior por que las empresas de mayor tamaño están ubicadas dentro de esa región y ellas tienen tanto unidad de auditoría interna como departamento de informática que fueron de suma importancia para llevar a cabo la investigación.

3.2.2 Temporal

El periodo de estudio comprendió desde el año 2014 hasta el mes de julio del año 2016, ya que a partir de esa fecha se vio el incremento en la necesidad de poseer controles sobre los procesos realizados en el departamento de tecnologías de información debido a que las filtraciones de datos confidenciales, así como ataques a servidores privados por parte de hackers informáticos está siendo una práctica común; es por esto que la unidad de auditoría interna debe poseer mayor información respecto a evaluaciones de la normativa aplicable al área informática, bajo el enfoque de buenas prácticas.

3.3 SUJETOS Y OBJETOS DE ESTUDIO.

3.3.1. Unidades de análisis.

El estudio se enfocó en las empresas comercializadoras de electrodomésticos, y se determinó como unidades de análisis el personal de la unidad de auditoría interna y el personal del departamento de informática de empresas clasificadas como medianas y grandes contribuyentes tomando como base los ingresos anuales de estas entidades, de las cuales el número de empresas que cuentan con ambos departamentos son 16 según la información obtenida en el Ministerio de Hacienda.

3.3.2. Población y marco muestral.

La población de estudio fueron las empresas dedicadas a la comercialización de productos electrodomésticos; según los estudios realizados por la DIGESTYC y la información obtenida en el Ministerio de Hacienda solo 16 empresas contaban con las características necesarias para realizar la investigación, el criterio tomado para la determinación de las empresas a investigar fue que estuviesen clasificadas como grandes y medianas contribuyentes, de las cuales la mayor cantidad están ubicadas en la zona metropolitana de San Salvador, debido a que el universo es una población finita, es decir que no excedía las 30 empresas, tanto para el universo como para la muestra se tomó el número de empresas antes mencionadas.

3.3.3. Variables e indicadores

1. Variables

Variable independiente: Elaborar programas para la realización de una evaluación al departamento de tecnologías de información.

Variable dependiente: cumplimiento de la normativa técnica en el manejo, uso y cuidado del sistema informático y sus componentes.

2. Indicadores de variable independiente:

a) Perfiles profesionales.

b) Conocimientos normativos en materia de tecnologías de información.

c) Capacitación del personal.

d) Planes de seguimiento.

e) Compromiso del gobierno corporativo.

f) Políticas de la entidad aplicables al uso de tecnologías de información.

3. Indicadores de variable dependiente:

a) Conocimientos normativos en materia de determinación de riesgos en las tecnologías de información.

b) Implementación de los programas.

3.4 TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN.

3.4.1 Técnicas y procedimientos para la recopilación de la información.

Se llevó a cabo la investigación con las siguientes técnicas:

Se realizó una encuesta al personal encargado de la unidad de auditoría interna y sus colaboradores, con el propósito de profundizar en la investigación y conocer de la experiencia y conocimientos que estos poseen.

3.4.2 Instrumentos de medición.

Los instrumentos que se utilizaron en la investigación fueron:

- Cuestionario, el cual contenía una serie de preguntas cerradas y de opción múltiple.

  Se formularon 20 preguntas cerradas, con el propósito de comprobar cada indicador. (Anexo 1)

3.5 PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN

3.5.1 Procesamiento de la información.

Posteriormente de la aplicación de las diferentes técnicas e instrumentos de investigación, con los datos obtenidos se hicieron uso de cuadros de análisis a través de la herramienta de Microsoft Excel, que ayudo a la interpretación y análisis de los resultados obtenidos.

3.5.2 Análisis e interpretación de los datos procesados.

El análisis consistió en la interrelación entre las diferentes variables, tanto la dependiente como la independiente, así como en la operacionalización de los indicadores.

Con base al análisis de la variable independiente y dependiente y la interacción de los distintos indicadores en el resultado de la encuesta se procedió a formular un diagnóstico.

3.6 CRONOGRAMA DE ACTIVIDADES

ACTIVIDADES DEL MES	JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
ACTIVIDADES																												
CAPÍTULO I																												
Situación Problemática																												
Marco teórico																												
Generalidades de la Investigación																												
Entrega final																												
CAPÍTULO II																												
Marco Referencial																												
Recopilación de la información																												
Entrega final																												
CAPÍTULO III																												
Realización de encuestas																												
Procesamiento y análisis de la información																												
Tabulación y análisis de resultados																												
CAPÍTULO IV																												
Elaboración de la propuesta																												
Esquema de guía																												
Realizar diseño de actividades para los programas																												
Integración de los capítulos																												
Entrega final																												

3.7 PRESENTACIÓN DE LOS RESULTADOS

3.7.1 TABULACIÓN Y ANÁLISIS DE LOS RESULTADOS

3. ¿Cuánto tiempo tiene de ejercer la auditoría interna?

Alternativa	**Fr.**	**Fr. %**
1) De 0 a 6 meses	2	13%
2) De 6 meses a 1 año	2	13%
3) De 1 a 3 años	8	50%
4) Más de 3 años	4	25%
	16	**100%**

Análisis:

Dentro de los aspectos a evaluar para el perfil del recurso humano de las unidades de auditoría interna esta la experiencia que poseen los auditores internos, esto marca un parámetro para realizar las actividades asignadas.

El tiempo de experiencia de los auditores influye de manera importante en las actividades de las unidades de auditoría interna debido a que una de las causas de porque no se realizan auditorías al área de tecnología de información es la falta de experiencia en este caso según la información recopilada, solo el 13% de los encuestados posee una experiencia de 0 a 6 meses en el aérea, sin embargo la mayoría de auditores internos posee una experiencia de 1 a 3 años dando como resultado que el 50% de los auditores entrevistados, los auditores con una mayor experiencia son de 25% de la población estudiada.

Esto nos da como resultado que el 75% de los auditores tienen una experiencia mayor a un año, teniendo así mayores conocimientos sobre auditoría interna, las buenas prácticas y por ente

tecnologías de información, sin embargo en los datos resultantes de las preguntas 5 y 6 nos da como resultado que efectivamente la mayoría de los encuestado conoce sobre la aplicación de las buenas prácticas en un 56%, pero estos conocimientos no se encuentran actualizados debido a que el 44% de los auditores recibió su última capacitación sobre el tema hace más de 3 años, dejando así conocimientos ambiguos así como nuevas técnicas y aéreas a evaluar como lo es el área de tecnologías de información

4. ¿Qué conocimientos tiene del área de informática y que le son aplicables en el contexto de su ejercicio?

Alternativa	**Fr.**	**Fr. %**
1) COBIT 5	8	35%
2) ISO	11	48%
3) ITAF	2	9%
4) Todas las anteriores y otras	2	9%
	23	**100%**

Para llevar a cabo una auditoría interna al área de tecnologías de información se necesita poseer conocimiento en normativa aplicable a dicha área, debido a que es un área especializada, dentro de los requerimientos para el perfil necesario dentro de la unidad de auditoría interna están los conocimientos en materia de tecnologías de información, ya que la falta de conocimiento de la normativa puede llegar a influir para la realización o no de las auditorías al departamento de tecnologías de información.

Entre la normativa aplicable que se necesita para realizar procedimientos de auditoría interna al área de tecnologías de información esta COBIT 5, ISO 27001 y 27002, e ITAF, no obstante

según los resultados de los encuestados solo el 9% de ellos posee conocimiento de estas normativas aplicables, la mayoría posee conocimiento sobre la normativa ISO, dejando con menores conocimientos las normativas COBIT 5 e ITAF; la falta de conocimiento y dominio de las tecnologías de información son parte de las causas por las cuales los auditores internos no realizan auditorías a este departamento, sin embargo según los resultados obtenidos en la pregunta nº7 los auditores encuestados han recibido capacitaciones sobre aéreas de tecnologías de información, en su mayoría sobre seguridad de la información.

5. ¿Conoce usted sobre la aplicación de las buenas prácticas al departamento de informática?

Alternativa	**Fr.**	**Fr. %**
Si	9	56%
No	7	44%
	16	**100%**

Análisis:

Dado que la auditoría interna es una actividad para generar valor y mejorar los procesos dentro de las empresas el conocimiento sobre la aplicación de buenas prácticas es de suma importancia para las unidades de auditoría interna.

Los resultados obtenidos de los encuestados en un 56% posee conocimientos sobre la aplicación de buenas prácticas al departamento de tecnologías de información versus un 44% que no posee conocimiento sobre ello, sin embargo en los obtenido en la pregunta Nº15 sobre la realización de

auditorías al área de tecnologías de información el 81% de estas empresas no llevan a cabo auditorías de este tipo, lo que podemos concluir que dichos conocimientos no son aplicados, por la falta de conocimiento sobre la normativa técnica como se observa en los resultados de la pregunta Nº4.

6. ¿Indique hace cuánto tiempo recibió su última capacitación en el área de buenas prácticas?

Alternativa	**Fr.**	**Fr. %**
1) De 0 a 6 meses	3	19%
2) De 6 meses a 1 año	3	19%
3) De 1 a 3 años	3	19%
4) Más de 3 años	7	44%
	16	**100%**

Análisis:

Para contribuir a los conocimientos y la aplicación de las buenas prácticas es necesario poseer actualizaciones constantes sobre el temas, no obstante la mayoría de auditores recibieron su última capacitación hace más de tres años en un porcentaje del 44%, lo cual es alarmante para llevar a cabo las actividades de auditoría interna de una manera desfasada y eso no contribuye al mejoramiento de los procesos dentro de la entidad; los demás encuestados respondieron en un 19% para cada opción haber recibido estas capacitaciones de 0 a 6 meses, de 6 meses a 1 años y de 1 a 3 años.

7. ¿Qué áreas de tecnologías de información y comunicación ha recibido en las capacitaciones?

Alternativa	Fr.	Fr. %
1) Seguridad Física	9	50%
2) Seguridad Lógica	2	11%
3) Redes y Comunicaciones	2	11%
4) Otras	5	28%
	18	**100%**

Análisis:

Dentro de los conocimientos obtenidos por los auditores internos por medio de capacitaciones en su mayoría ha sido en seguridad física a las tecnologías de información que consta sobre el uso y cuidado que debe poseer al uso de tecnologías de información en un 50% de los entrevistados respondió haber recibido capacitaciones sobre esta área, dejando con un 11% capacitaciones sobre seguridad lógica y redes y comunicaciones, y en un 28% en otras capacitaciones sobre este tema, esto con el objetivo de medir que tan involucrada se encuentra la gerencia sobre la importancia de que los auditores estén en actualización constante de los conocimientos necesarios para llevar a cabo las actividades de auditoría en el área de tecnología de información.

8. ¿El acceso a los sistemas se encuentra jerarquizado?

Alternativa	**Fr.**	**Fr. %**
Si	7	44%
No	9	56%
	16	**100%**

Análisis:

Debido que este tipo de empresas manejan por medio de sistemas computarizados sus operaciones es necesario que dichas compañías posean políticas de seguridad no solo física sino que también de manera lógica dentro de ellas, para proteger la información que carácter confidencial, así como registros, modificaciones entre otras como las intrusiones no deseadas al sistema las empresas deben contar con medidas de seguridad como la jerarquización de los sistemas la mayoría en un 56% de los encuestados respondieron no contar con jerarquización de los sistemas dejando libre acceso a los empleados sobre los datos del sistema.

9. ¿Con que frecuencia la alta dirección participa en eventos relacionados con el sistema de gestión de la seguridad informática?

Alternativa	Fr.	Fr. %
1) Mensualmente	2	13%
2) Cada seis meses	3	19%
3) Una vez al año	6	38%
4) Nunca participa	5	31%
	16	100%

Análisis

La seguridad informática es un factor del cual los gerentes deben de estar muy pendientes, ya que una falla en el sistema informático conlleva muchos riesgos entre los cuales se pueden mencionar, perdida de información confidencial, virus informáticos que afecten los ordenadores, error en procesos importantes, entre otros, por este motivo el gobierno corporativo debe poseer especial compromiso en el seguimiento al departamento de tecnologías de información.

Según la investigación realizada se determinó que solo un 13% de las empresas efectúan eventos los cuales están relacionados con la seguridad informática, es decir, para estas empresas es de suma importancia la realización y seguimiento de evaluaciones continuas al departamento de tecnologías de información, no siendo así para un 31% de las entidades encuestadas ya que estas nunca ejecutan procedimientos encaminados a la seguridad de la información, por otro lado, un 19% de las compañías toman en cuenta la seguridad informática ya que por lo menos cada 6 meses están en constante seguimiento en esta área, por ultimo podemos identificar que las organizaciones en las que sus gerentes participan en eventos relacionados a la seguridad de la información es un 38% del total de encuestados.

10. ¿Qué tan consiente se encuentra el personal de auditoría interna de los objetivos del departamento de informática?

Alternativa	Fr.	Fr. %
a) Muy consiente	0	0%
b) Consiente	15	94%
c) No conoce los objetivos	1	6%
	16	100%

Análisis

El departamento de auditoría interna por ser uno de sus roles la evaluación total de las empresas deben conocer los objetivos que persigue cada área de la entidad para poder realizar los

procedimientos necesarios a la hora de ejecutar la auditoría como tal y plantear planes de seguimiento para cada departamento.

De los resultados que genero la realización de encuestas se puede observar que con un 94% la mayoría de las empresas poseen conciencia y conocimiento de los objetivos que persigue el departamento de tecnologías de información, en cambio un 6% que corresponde de las entidad encuestadas no conoce las objetivos del departamento.

11. ¿Posee el software más adecuado para el manejo de la información de los clientes?

Alternativa	Fr.	Fr. %
Si	11	69%
No	5	31%
	16	100%

Análisis

Uno de los factores que se evalúan al momento de la verificación de la seguridad de la información es el software que las empresas utilizan en sus labores cotidianas, poseer un software actualizado y seguro debe ser un política empresarial respecto al uso de las tecnologías de información para poder obtener los mejores resultados posibles y poseer la mayor confidencialidad de los datos de los clientes.

De las entidades encuestadas un 69% contesto que ellas poseen un software adecuado para el manejo de la información de los clientes lo que repercute en una buena administración de los datos confidenciales y de los procesos realizados, por otro lado se puede observar que un 31% no poseen el software más adecuado lo que debilita la seguridad y existe un mayor riesgo para la información.

12. ¿Con qué frecuencia se realizan revisiones para determinar y eliminar causas de posibles daños a la entidad?

Alternativa	Fr.	Fr. %
1) Mensualmente	1	6%
2) Cada seis meses	2	13%
3) Una vez al año	11	69%
4) Nunca	2	13%
	16	100%

Análisis

La auditoría interna debe tener constante seguimiento sobre los riesgos que puedan afectar a la entidad es por ello que se deben realizar constantemente evaluaciones que determines amenazas y que se puedan eliminar de forma adecuada.

Los resultados que dio la investigación determinó que un su mayoría y con un 69% las empresas realizan revisiones anualmente lo cual vulnera la seguridad de la información ya que no es posible identificar con suficiente tiempo amenazas que pueden afectar a la entidad, por otro lado se observa que un 13% de las empresas efectúan revisiones cada 6 meses y también un 13% de las entidades encuestadas nunca realizan revisiones para la determinación de posibles daños, de todos los encuestados solamente un 6% respondió que se ejecutan revisiones mensualmente, lo cual garantiza un mayor control de los riesgos y la determinación anticipada de las amenazas que afecten a la organización.

13. ¿Qué tan frecuente son tomados en cuenta los procesos importantes y tareas en los programas de auditorías realizados?

Alternativa	Fr.	Fr. %
1) Siempre son tomadas en cuenta	2	13%
2) Frecuentemente son tomadas en cuenta	12	75%
3) Nunca son tomados en cuenta	2	13%
	16	100%

Análisis

Los procesos importantes dentro de cada departamento de la empresa deben ser tomados en cuenta para realizar los programas de auditoría ya que de esta manera se sabe a qué tomarle mayor importancia y a que procesos se le debe dar mayor seguimiento.

Según los resultados de la encuesta un 75% de las empresas investigadas toman en cuenta frecuentemente los procesos y las tareas importantes del departamento de tecnologías de información, mientras que con 12.5% los auditores internos en la elaboración de los programas utilizados toman en cuentan los procesos importantes, así mismo con un 12.5% de las empresas encuestadas, los auditores internos no toman en cuenta los procesos y tareas del departamento de informática.

14. ¿Qué tan documentados están los registros del proceso de auditoría interna?

Alternativa	Fr.	Fr. %
1) Muy bueno	3	19%
2) Bueno	11	69%
3) No están documentados	2	13%
	16	100%

Análisis

Para todos los programas de auditoría que se ejecuten en cada revisión estos deben ser evidenciados por documentos de respaldos e información que ayuden a sustentar todos los procedimientos que el auditor realizo.

Según los datos recabados en la ejecución de las encuestas observamos que un 19% poseen un muy buen respaldo de los procedimientos efectuados, por otra parte y con un 69% los auditores internos respondieron que sus procedimientos están documentados de una forma buena, y con un 13% de respuestas se observa que los procesos de auditoría no están documentados en ninguna forma.

15. ¿Se realizan auditorías internas al departamento de tecnologías de información?

Alternativa	Fr.	Fr. %
Si	3	19%
No	13	81%
	16	100%

Análisis:

En el ámbito de conocimiento de los auditores en las buenas prácticas deben conocer acerca de la aplicación de programas que les ayuden a evaluar al área de informática.

Al observar los resultados obtenidos con los auditores encuestados se puede visualizar que el 81% de estos auditores no realizan auditorías al departamento de informática por falta de programas, interés por porte de la administración, entre otras causas; y solo un 19% respondió que realiza auditorías a esta área.

16. ¿Qué tan frecuentemente se realizan auditorías internas al departamento?

Alternativa	**Fr.**	**Fr. %**
1) Cada año	2	13%
2) Cada dos años	1	6%
3) Tres años o más.	0	0%
	3	19%

Análisis:

Con el conocimiento de buenas prácticas, los auditores cuentan con las herramientas necesarias para realizar un seguimiento de las auditorías en los distintos departamentos de las empresas.

El realizar auditorías a las diferentes áreas de la empresa es muy importante para verificar el adecuado funcionamiento de cada una de estas áreas, al encuestar a los auditores la frecuencia con la que realizan auditorías al área de tecnologías de información, se pudo observar que en su

mayoría los auditores se abstuvieron a responder la pregunta, mostrando así que en su mayoría los auditores dejan de lado la evaluación a dicho departamento.

En los resultados obtenidos se pudo obtener que solo un 19% respondió a la interrogante, de los cuales un 13% auditores realizan auditorías anual mente y un 6% realiza auditorías cada dos años; mientras que un 81% se abstuvo a contestar la pregunta.

17. ¿El departamento de auditoría interna posee periodos establecidos para la realización de auditorías internas a la unidad de tecnologías de información?

Alternativa	**Fr.**	**Fr. %**
1) Cada mes	0	0%
2) Semestralmente	0	0%
3) Anual	5	31%
4) Nunca	8	50%
	13	81%

Análisis:

El cuidado de los activos tecnológicos que posee la empresa es uno de los aspectos que el departamento de auditoría interna debiera verificar, debido a la importancia que representa este activo al momento de administrar los créditos otorgados y la información que se maneja de los clientes.

En los resultados obtenidos con los encuestados se pudo observar que el 50% no posee periodos establecidos para realizar auditorías al departamento de T.I.; así mismo un 19% se abstuvo de responder lo cual indica que tampoco poseen periodos para evaluar a dicha área y solo un 31% cuenta con periodos establecidos para evaluar a dicha área los cuales se realizan anualmente.

18. ¿Qué tan frecuente se realizan auditorías internas del sistema de gestión de la seguridad de la información (SGSI) en los periodos establecidos?

Alternativa	**Fr.**	**Fr. %**
1) Cada mes	0	0%
2) Semestralmente	1	6%
3) Anual	8	50%
4) Nunca	7	44%
	16	100%

Análisis:

Los auditores deben poseer conocimientos en distintas áreas debido a la complejidad que cada una posee, uno de los conocimientos que se requieren al evaluar al departamento de T.I. son en la determinación de los riesgos que conlleva esta área por la vulnerabilidad de la tecnologías cambiantes y amenazas que existen en la web.

Los resultados obtenidos a través de la investigación arrojan resultados en los cuales se puede evidenciar que en su mayoría los auditores realizan en la seguridad de información en periodos anuales arrojando un porcentaje del 50%, pero también se observa que de igual manera un 44% nunca realiza una auditoría de este tipo y solo un 6% realiza auditorías de este tipo semestralmente.

19. ¿Se cuentan con procedimientos que evalúen el uso, cuidado y mantenimiento de los activos tecnológicos de la empresa?

Alternativa	Fr.	Fr. %
Si	6	38%
No	10	63%
	16	100%

Análisis:

Uno de los cuidados que se deben poseer en el área de informática para resguardar la información con que se cuenta es el acceso a los sistemas por parte de los empleados, el departamento de auditoría debe evaluar los accesos y cuidados de los equipos tecnológicos con que cuenta el área de tecnologías de la información.

El 63% de los auditores afirmaron que no poseen procedimientos que les ayuden a evaluar al departamento de informática en las empresas, dificultando esto la evaluación de dicha área; así mismo un 38% respondió que cuentan con programas para evaluar el área, sin embargo los mismos no son aplicados, ya que en relación a la interrogante N° 15 se estableció que no se realizan auditorías al departamento de tecnologías de la información.

20. ¿Estaría usted dispuesto a utilizar una propuesta de los programas de auditoría interna que contemplen la evaluación de T.I. bajo el enfoque de buenas prácticas?

Alternativa	**Fr.**	**Fr. %**
Si	15	94%
No	1	6%
	16	100%

Análisis:

Los auditores necesitan herramientas que los ayuden a realizar de forma óptima sus labores diarias, es por eso que se ven en la necesidad de contar con procedimientos que ayuden a evaluar de forma adecuada al departamento de informática de la empresas, así también evaluar el riesgo y vulnerabilidades que este mismo posee con el crecimiento constante de la tecnología y el alto grado de amenazas que surgen día con día.

En los resultados obtenidos con la encuesta se pudo obtener que un 94% de la población encuestada se encuentra interesada en la propuesta de programas para evaluar al departamento de tecnologías de la información, así mismo estarían dispuestos a utilizarlas en sus evaluaciones y solo un 6% respondió que no se encuentra interesado en dichos programas.

3.7.2 DIAGNÓSTICO DE LA INVESTIGACIÓN

De los resultados que se obtuvieron de los encuestados se tomaron los puntos de mayor prioridad que ayudaron a cumplir con el propósito planteado para la investigación, esto con el fin de crear una herramienta que facilite al auditor interno realizar auditorías a la normativa técnica aplicable al área de tecnologías de información que comprende Hardware, Software, Seguridad física y seguridad lógica, en el departamento de informática en las empresas de comercialización de electrodomésticos del área metropolitana de San Salvador.

El diagnóstico de la investigación para poder analizar las variables se dividió en las siguientes áreas:

Tabla 1: Evaluación al perfil de recurso humano que se desempeña en las unidades de auditoría interna.

Nº de pregunta	**Alternativa**	**Frecuencia**	
		Absoluta	**Relativa**
3	Tiempo de experiencia que tienen los profesionales encuestados en el área de auditoría interna		
	• De 0 a 6 meses	8	50%
	• De 6 meses a 1 año	4	25%
9	Frecuencia en que la alta dirección se participa en eventos relacionados con el sistema de gestión de la seguridad informática		
	• Una vez al año	6	38%
	• Nunca participa	5	31%
10	Grado de conocimiento que posee el personal de auditoría interna sobre los objetivos del departamento de informática		
	• Consiente	15	94%
	• No conoce los objetivos	1	6%
4	Conocimientos que poseen los auditores internos encuestados sobre el área de informáticos que son aplicables en el desarrollo del ejercicio de auditoría interna		
	• COBIT 5	8	35%
	• ISO	11	48%
	• ITAF	2	9%
	• Todas las anteriores y otras	2	9%

El recurso humano dentro de las empresas es una pieza clave para llevar a cabo la realización de los diversos procesos dentro ella, siempre y cuando se cuente con el personal idóneo para el desarrollo de las actividades, sin embargo el personal se las unidades de auditoría

interna según los datos obtenidos del estudio realizado cuentan con poca experiencia sobre el área un 75% de los profesionales encuestados poseen una experiencia entre 0 meses y un año, añadiendo a ello dentro de las limitantes el bajo nivel de participación que tiene la alta gerencia en eventos relacionados al sistema de gestión de la seguridad informática en su mayoría la frecuencia con que se involucra la gerencia es una vez al año en un 38% y en un 31% no participa en ninguna ocasión, sin embargo la mayoría de los entrevistados esta consiente en 94% de los objetivos del departamento de informática, no obstante el 6% de los encuestados no conoce los objetivos.

En consecuencia que los auditores internos que se desempeñan en las unidades de auditoría interna cuentan con poca experiencia y añadiendo a esto los pocos conocimientos que poseen los auditores internos en normativa aplicable al área de tecnologías de información según el estudio realizado un 35% de los encuestados respondieron tener conocimiento sobre COBIT 5, normas de calidad ISO con un 48% hace mención que conoce sobre ello, un 9% de los profesionales respondieron que poseen conocimientos sobre ITAF, sin embargo solamente el 9% manifiesta que conoce todas normativas antes mencionadas lo cual no es representativo debido que corresponde solamente a dos de los encuestados.

Tabla 2: El nivel de capacitación que está recibiendo el recurso humano.

Nº de pregunta	**Alternativa**	**Frecuencia**	
		Absoluta	**Relativa**
7	Áreas de tecnologías de información y comunicación en las cuales han recibido capacitación los auditores		
	• Seguridad Física	9	50%
	• Seguridad Lógica	2	11%
	• Redes y Comunicaciones	2	11%
11	El software para el manejo de la información de los clientes es el adecuado		
	• Si	11	69%
	• No	5	31%
12	Frecuencia con que se realizan revisiones para determinar y eliminar causas de posibles daños a la entidad		
	• Una vez al año	11	69%
	• 4) Nunca	2	13%

Los encargados de desempeñar la función de auditores internos en las empresas comercializadoras de electrónicos a pesar de tener un rango de entre 0 y 3 años de desempeñar el cargo ya poseen capacitaciones respecto a áreas de tecnologías de información y comunicaciones, específicamente en áreas de seguridad física en 50%, en seguridad lógica un 11% , redes y telecomunicaciones también un 11%, pese a que las capacitaciones no son en su mayoría en seguridad lógica, los encuestados en un 69% consideran que el software que utilizan en sus entidades es el más adecuado en seguridad y esta actualización respecto a las necesidades que posee el negocio además de que el software es el que mejor se desempeña en el manejo de información de los clientes, por otro lado un 31% de la población encuestada revela que para

ellos el software que se utiliza en sus compañías no es el más idóneo para realizar las actividades diarias que se efectúan.

Los encuestados al no poseer una actualización constante respecto a seguridad lógica, redes y telecomunicaciones, no están facultados de una manera idónea para efectuar revisiones que detecten y eliminen causas de posibles daños a la entidad, y al ser una de las vías de ataque el ciberespacio, las entidades se encuentran amenazadas con posibles ataques que dañen desde una computadora hasta perder toda una base de datos de clientes que la compañía no tenga respaldada de una manera correcta, ya que según las respuestas reveladas por los encargados del departamento de auditoría en un 69% realizan revisiones preventivas anualmente, y un 13% nunca realizan este tipo de verificaciones teniendo aun un mayor grado de vulnerabilidad a las amenazas que pueden presentarse.

Tabla 3: Evaluar con qué frecuencia el personal recibe capacitaciones en buenas prácticas.

Nº de pregunta	Alternativa	Frecuencia	
		Absoluta	**Relativa**
	Tiempo en que los profesionales encuestados han recibido su última capacitación en el área de buenas prácticas.		
	• De 1 a 3 años	3	19%
	• Más de 3 años	7	44%

La actualización constante de los conocimientos que poseen profesionales sobre la aplicación de buenas prácticas al área de tecnologías de información, es de suma importancia para el buen desempeño en la realización de las actividades de auditoría, sin embargo los auditores internos encuestados en un 19%, manifiestan haber recibido su última capacitación en un intervalo de tiempo de 1 a 3 años, más alarmante aun un 44% de los profesionales respondieron que su última capacitación recibida sobre el tema fue hace más de tres años que representa 7 de los auditores encuestados, bajo esta información obtenida podemos afirmar que los conocimientos que poseen no son los idóneos para llevar a cabo la auditoría interna bajo el enfoque de buenas prácticas, por tanto se ha dejado de lado nuevas técnicas de auditoría así como también nuevos departamentos a examinar o departamentos que están en constante cambio, como es el caso del departamento de tecnologías de información, que al encontrarse en constante cambio los auditores deben estar capacitándose periódicamente para llevar a cabo las actividades de auditoría de manera eficiente de acuerdo a lo que se presenta actualmente y esto contribuye a que el desarrollo de las mismas le agregue valor a los procesos establecidos y se cumpla con los objetivos.

Tabla 4: Verificar si los auditores internos aplican en su trabajo de auditoría las buenas prácticas.

Nº de pregunta	Alternativa	Frecuencia	
		Absoluta	Relativa
5	Conocimientos del personal en la aplicación de las buenas prácticas al departamento de informática • Si • No	 9 7	 56% 44%
13	Frecuentemente son tomados en cuenta los procesos importantes y tareas en los programas de auditorías realizados • Frecuentemente son tomadas en cuenta • Nunca son tomados en cuenta	 12 2	 75% 13%
14	Documentación correcta de los proceso de auditoría interna • Buena • No están documentados	 11 2	 69% 13%
15	Realización de auditorías internas al departamento de tecnologías de información • Si • No	 3 13	 19% 81%
16	Frecuentemente se realizan auditorías internas al departamento de informática • Cada año • Cada dos años • Tres años o más.	 4 1 0	 80% 20% 0%

20	Interés que muestran los profesionales encuestados en utilizar una propuesta de los programas de auditoría interna que contemplen la evaluación de T.I. bajo el enfoque de buenas prácticas • Si • No	 15 1	 94% 6%

La tecnología sufre constantes cambios en la actualidad, creando innovaciones que facilitan el trabajo en distintas áreas de las empresas, es por ello que se vuelve necesario contar con herramientas necesarias para evaluar las innovaciones tecnológicas con las que cuenta el departamento de tecnologías de información y comunicación; En su mayoría los auditores poseen conocimientos sobre las buenas prácticas con un porcentaje de 56%, sin embargo el 44% desconoce de las mismas.

En el desarrollo de los procesos importantes y tareas que realizan las empresas se vuelve necesario tomar en cuenta cada uno de ellos en la realización de los programas de auditoría para lograr un desarrollo óptimo de los mismos, en tal sentido dichos procesos son tomados frecuentemente en cuenta según el 75% de los encuestados, mientras que el 13% afirmo que nunca son tomados en cuenta al momento de la elaboración de los programas; De igual forma con base a la escaza frecuencia con que se encuentra involucrada la administración en eventos relacionados con el sistema de gestión de la seguridad informática la realización de auditorías al departamento de informática se vuelve necesaria para evaluar las vulnerabilidades a las que se encuentra expuesto el departamento, sin embargo en los resultados que se obtuvieron por parte de los profesionales encuestados el 81% manifiesta que no realizan auditorías internas al área de

T.I. de las empresas, llevando esto a la posible pérdida de información vital para las entidades, así mismo 19% de los profesionales encuestados si realizan auditorías al área antes mencionada; en la realización de las evaluaciones al departamento de informática se llevan a cabo anualmente según lo manifestó un 80% dificultando la prevención a las constantes amenazas que se encuentran en la red informática, además un 20% solo realizan auditorías cada dos años sin avaluar las distintas amenazas hacia las empresas.

Debido a la falta de interés de la administración, los escasos conocimientos que poseen el personal de las unidades de auditoría y la escasa evaluación que se realizan a los procesos del departamento de informática, los profesionales encuestados están interesados en utilizar una propuesta de los programas de auditoría interna que contemplen la evaluación de T.I. bajo el enfoque de buenas prácticas en un 94%, no obstante el 6% de los encuestados no manifiesta interés en la aplicación de los programas.

Tabla 5: Evaluar si el personal cumple con los lineamientos y procedimientos en el caso de uso, cuidado y mantenimiento del activo tecnológico.

Nº de pregunta	Alternativa	Frecuencia	
		Absoluta	**Relativa**
17	Periodos establecidos para la realización de auditorías internas a la unidad de tecnologías de información • Anual • Nunca	 5 8	 38% 62%
18	Frecuentemente se realizan auditorías internas del sistema de gestión de la seguridad de la información (SGSI) en los periodos establecidos • Anual • Nunca	 8 7	 50% 44%
19	Existencia de procedimientos que evalúen el uso, cuidado y mantenimiento de los activos tecnológicos de las empresas • Si • No	 6 10	 38% 63%
8	Controles de acceso a los sistemas de forma jerarquizada • Si • No	 7 9	 44% 56%

Con los constantes crecimientos tecnológicos que existen en la actualidad uno de los cuidados que se deben poseer en el área de informática para resguardar la información con que se cuenta es el acceso a los sistemas por parte de los empleados, el departamento de auditoría debe evaluar los accesos y cuidados de los equipos tecnológicos con que cuenta el área de T.I, restringiendo así el acceso del personal a los diferentes sistemas y áreas, contando con accesos jerarquizados en el ingreso y uso de la información, siendo así el 56% de los profesionales no cuentan con acceso jerarquizados, vulnerando esto en gran medida la seguridad de los equipos

informáticos de igual manera el 44% de los encuestados si posee jerarquizados los accesos a los sistemas; Los auditores deben poseer conocimientos en las distintas áreas debido a la complejidad que cada una posee, uno de los conocimientos que se requieren al evaluar al departamento de T.I. es en la determinación de los riesgos que conlleva esta área por la vulnerabilidad de la tecnologías cambiantes y amenazas que existen en la web siendo necesarios contar con periodos establecidos para la realización de auditorías a la unidad de tecnologías de la información con un 38% que establece periodos anuales de evaluación, mientras que el 62% nunca establecen periodos para evaluar a la unidad de informática.

Debido a la falta de periodos establecidos para realizar auditorías a la unidad de informática y distintos factores que evitan la realización frecuente de auditorías internas del sistema de gestión de la seguridad de la información (SGSI) en un 44% a su vez el 50% realizan este tipo de auditorías anualmente, no siendo los periodos más adecuados para dicha realización; además las empresas deben poseer en el área de informática cuidados para resguardar la información con que se cuenta contando con procedimientos que evalúen el uso, cuidado y mantenimiento de los activos tecnológicos de las empresas contando con ellos solo el 38% de los encuestados, siendo un porcentaje por debajo de la mitad de los profesionales encuestados debido a que un porcentaje de 63% afirmo que no poseen procedimientos para evaluar el cuidado de dichos activos.

4 CAPÍTULO IV: PROPUESTA DE SOLUCIÓN

PROGRAMAS DE AUDITORÍA INTERNA PARA REALIZAR UNA EVALUACIÓN AL ÁREA DE TECNOLOGÍAS DE INFORMACIÓN BAJO EL ENFOQUE DE BUENAS PRÁCTICAS EN LAS EMPRESAS COMERCIALIZADORAS DE ELECTRODOMÉSTICOS UBICADAS EN EL ÁREA METROPOLITANA DE SAN SALVADOR.

4.1 PLANTEAMIENTO DEL CASO

En este capítulo se presenta una propuesta de lo que debe contener un plan de auditoría para evaluar al área de tecnologías de información en las empresas comercializadoras de electrodomésticos bajo el enfoque de buenas prácticas.

Para la realización de los programas de auditoría interna que evalúen al área de tecnologías de información se necesita llevar a cabo el conocimiento preliminar de la empresa para determinar los posibles riesgos que pueden afectar a la entidad, dentro de ello podemos mencionar principios y valores que posee la empresa, productos que comercializan, estructura organizativa, áreas de negocio y las funciones que esta realiza entre otros.

Se lleva a cabo un memorándum de planeación para la evaluación del departamento de auditoría interna en la cual se desarrolla el alcance de la auditoría, los objetivos que esta persigue, asignación de recursos y los programas de trabajo.

Las empresas antes mencionadas realizan ventas al por mayor y al detalle a través de sucursales ubicadas en centros comerciales o en puntos estratégicos de la región generando altos índices de crédito, actualmente se cuenta con servicio de tienda en línea proporcionando facilidades a los clientes para adquirir los productos que estas empresas ofrecen.

4.2 DESARROLLO DEL CASO PRÁCTICO

4.2.1 CONOCIMIENTO PRELIMINAR

CONOCIMIENTO DE LA EMPRESA: ALMACENES SI VAN, S.A. DE C.V.

a) Giro: Venta de electrodomésticos

b) Constituida: La referida sociedad, se constituyó por medio de Escritura Pública, otorgada en la ciudad de San Salvador, a las quince horas del día 27 de septiembre de 1999, ante los oficios notariales de Héctor Alejandro Mejía Escobar, inscrita en el Registro de Comercio, el día 19 de octubre del mismo año, al número 53 folios 473 al 502 del libro 1474 del Registro de Sociedades

c) Capital social mínimo de fundación: ¢ 20,000.00 equivalente a $ 2,285.71

d) Naturaleza: Sociedad Anónima de Capital Variable

e) Domicilio: Kilómetro 28 ½ Carretera a Santa Ana, Municipio de San Juan Opico, Departamento de La Libertad

f) Plazo: Indefinido

g) Sucursales: Galerías, Metrocentro, La Gran Vía, Plaza Mundo, San Miguel, Santa Ana

h) Productos

Tabla 6: Principales productos comercializados.

Artículos de línea blanca:	Artículos de audio y video	Accesorios
• Lavadora	• Consolas de videojuego	• Teléfonos Inalámbrico
• Aires acondicionados	• Cámaras de video	• Teléfonos
• Refrigeradoras	• Cámaras digitales	• Cables de poder
• Secadora	• DVD	• Cables USB
• Microondas	• Teatros en casa	• Control remoto
• Tostadoras	• Equipos de sonido	
• Hornos	• Televisores	
• Estufas	• Radio grabadoras	

i) Misión

Superar las expectativas de nuestros clientes, brindándoles la mejor experiencia de compra, creando valor para nuestros colaboradores, accionistas y proveedores, con responsabilidad social.

j) Visión

Ser el Grupo detallista líder e innovador en los mercados donde operemos, diferenciándonos por ofrecer las últimas tendencias, un servicio extraordinario y siempre fieles a nuestros valores.

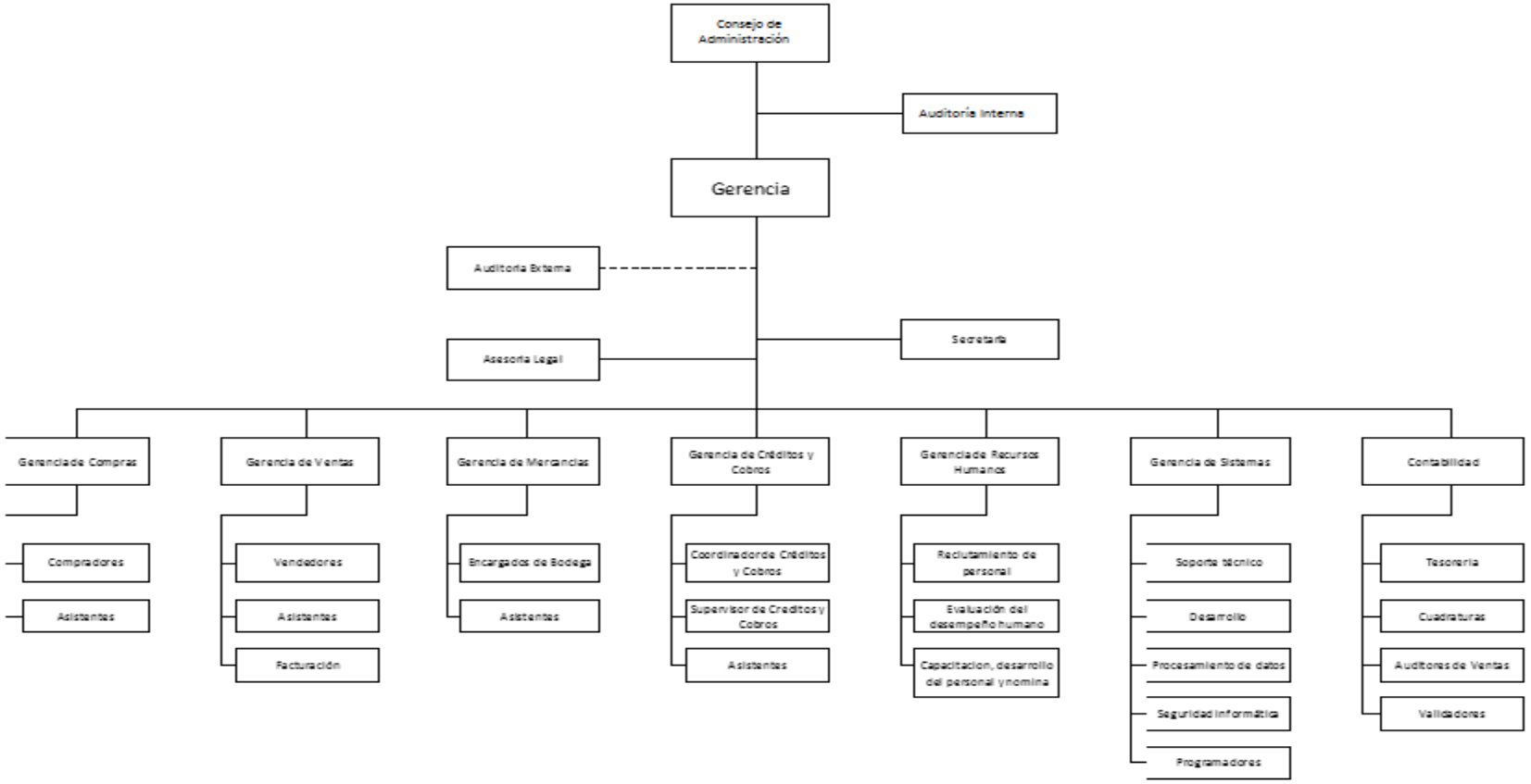
k) Principios y valores de la empresa

- Formalidad
- Cultura de servicio
- Creación de valor
- Ser parte del equipo
- Ética
- Respeto por las personas
- Honestidad
- Lealtad

ESTRUCTURA ORGANIZATIVA

El grupo empresarial cuenta actualmente con un aproximado de quinientos empleados a lo largo de toda la organización, tanto en el nivel operativo como en el administrativo. La estructura organizacional del grupo es de tipo vertical con varios departamentos y niveles de jerarquía.

Figura 1: Organigrama de la empresa.



ÁREAS DE NEGOCIO

a) Compras

Función general del Departamento de Compras

La función general del departamento es la de planificar, dirigir y controlar las actividades operacionales, administrativas y logísticas relacionadas con los procesos de compra, importación, almacenaje, promoción, transporte y elaboración de inventarios de la mercadería que posee la empresa.

Descripción de las unidades operativas administradas por el departamento de compras

Las unidades que maneja el departamento son las siguientes:

- Compras locales
- Importaciones
- Planificación
- Transporte
- Bodega

Cada una de las unidades tiene distintas funciones generales y específicas, pero sólo se describirá aquellas funciones específicas que afectan de alguna manera la administración de la bodega matriz.

b) Ventas

Función general del departamento.

La función del departamento es planear, ejecutar y controlar las actividades en este campo. Debido a que durante el desarrollo de los planes de venta ocurren muchas situaciones, el departamento de ventas debe de dar seguimiento y control continuo a las actividades de venta.

Funciones específica

- Elaborar pronósticos de ventas
- Establecer precios
- Realizar publicidad y promoción de ventas
- Llevar un adecuado control y análisis de las ventas

c) Contabilidad

Función general del departamento.

Llevar de manera técnicamente apropiada y actualizada, los libros y otros registros contables, realizando eficientemente el control y registro operativo de las operaciones contables, para que se refleje en los libros la situación financiera de la empresa, que permita a los jefes de cada departamento tomar decisiones oportunas y eficaces.

Funciones específica

- Control de la contabilidad
- Gestión de los costes

- Presupuestos
- Planes de inversión
- Planes de financiación
- Gestión del riesgo
- Políticas de reparto de dividendos

d) Mercancías

Función general del departamento.

Planificar, organizar y supervisar los procesos de recepción, almacenamiento, despacho y transferencia de la mercadería desde la bodega matriz hacia las bodegas de almacén o domicilios de los clientes.

Funciones específica

- Controlar el ingreso y egreso del inventario de mercadería existente en bodega.
- Realizar la aprobación de transferencias de mercadería hacia los almacenes.
- Coordinar la seguridad del estado de los activos.
- Organizar la bodega de acuerdo a técnicas de almacenamiento, optimizando espacios.
- Programar y coordinar con los colaboradores las actividades de despacho de mercadería.
- Participar y coordinar el desarrollo de inventarios físicos con el equipo de trabajo.

- Participar en la recepción y verificación de la mercadería tanto local como importada.
- Coordinar actividades con los proveedores de servicio técnico.
- Cumplir y hacer cumplir las normas de seguridad del área de bodega.
- Coordinar con el área de transporte el envío y recepción de mercadería.
- Coordinar con las jefaturas de agencia el tráfico de la mercadería.
- Coordinar con el área de control y entrega el correcto despacho de la mercadería.
- Mantener coordinación interna con la gerencia de operaciones.

e) Sistemas

Funciones específica

- Se encarga de desarrollar un sistema informático que permita a la empresa, un adecuado control de todos los procesos que se dan en la empresa
- Revisión continúa de los equipos

f) Créditos y cobros

Funciones

- Demostrar precisión en el análisis de capacidad de pago de clientes objetivos (personas de ingresos bajos y medios) en el seguimiento del crédito y la gestión de cobros antes y después del vencimiento de las cuotas.
- El otorgamiento del financiamiento a un cliente se realiza siguiendo la política de créditos de la empresa.
- El cliente debe llenar una serie de requisitos para otorgar el crédito, contar con referencias comerciales, información sobre ingresos y créditos.
- La gestión de cobros es realizada por un equipo entrenado específicamente para dicho efecto.
- Una cuenta que presenta mora pasa al departamento de gestión de cobros luego de cierto tiempo de atraso del cliente, en la medida que la probabilidad de no pago se incrementa, esta es derivada al departamento legal o cobranza judicial.

g) Recursos Humanos

Función general del departamento.

Formular y proponer al Gerente General técnicas de reclutamiento, motivación y capacitación del personal, de tal manera que la empresa obtenga y mantenga al recurso humano calificado y con la disposición necesaria para la eficiente ejecución de las actividades de trabajo y el mantenimiento de un ambiente de relaciones interpersonales de trabajo adecuado.

Procedimientos importantes

Proceso de compra

1. Inicialmente se establece una relación comercial con el proveedor en la cual ese realiza la presentación de sus productos y precios la cual se encarga el comprado y el asistente esta involucrados conjuntamente.

2. Luego se procede a realizar la proforma de la orden de compra la cual es desarrollada por el asistente de compra y enviada al digitador de mercancías posteriormente esta orden es aprobada por el supervisor de los digitadores.

3. Luego el asistente es confirmado la creación de orden de compra este deberá de enviarla al proveedor con las indicaciones sobre cual son las fechas iniciales para entrega y la fecha límite de la recepción de la mercancía.

4. El asistente luego de enviar la orden al proveedor deberá de darle seguimiento a todas las órdenes de compra que espera que se recepciones en el mes están incluyen las ordenes locales y las importadas

5. Dentro de este seguimiento deberá investigar el estatus de cada orden ya sea que sean importadas deberá estar al tanto de si la mercancía ya salió del país de origen, el tipo de transporte en que viene si en vía marítima o aérea, si en caso ya arribaron puerto conocer su estatus aduanero si están en recinto fiscal, si ya pago impuesto por la mercadería, si ha pasado el proceso de selectividad, se ya está en el centro de distribución de la empresa. Algo muy importante todo mercadería que viene importada inicialmente ingresa a ES luego esta enviada a los demás país (GT, NI y

CR), luego de ser enviada a los demás países se le sigue dando seguimiento a las ordenes hasta que estas sean ingresadas a cada tienda.

6. Un dato muy importante cada comprador tiene asignado un presupuesto el cual debe de utilizar para sus compras del mes al final de dicho mes se realiza una evaluación sobre las ventas si han dado la rentabilidad esperada además se evalúa si todo las ordenes que se habían planificado ingresaron en el mes correspondiente.

7. Un proceso importante dentro de la compra es que todo mercadería que será ingresada el proveedor deberá de enviar sus facturas a los departamentos de facturación local e importado para que dicho departamento realiza su proceso de facturación en el sistema esta procedimiento se realiza que se cuadra la orden de compra enviada previamente al proveedor y la factura presentada por el proveedor si todo esta correcto se dará autorización por dicho departamento y el proveedor y el asistente de compra serán informados así mismo también el departamento de recibo de mercadería el cual le entregara al proveedor viñetas y posteriormente le dará una fecha para que este pueda entregar la mercadería. Algo muy importante es que si existente diferencia en costos entre la factura y la orden de compra el departamento de facturación informara y el proveedor y el asistente de compra deberán de informar el monto correcta ya sea que se tenga que modificar la orden de compra en el sistema de la empresa o el proveedor tenga que enviar una nueva factura.

   En el caso de lo importado el departamento de importado enviará al departamento de facturación importado los retaceos en los cuales esta compuestos por una serie de ordenes en las cuales se ha realizado el prorrateo de los gastos relacionados a la

importación, si todo esta correcto se confirma y dicha mercadería puede ser enviada a las tiendas en el caso ES y en el caso de los países esta es enviada a los demás país ya sea por vía área o terrestre para el centro de distribución de cada país y luego a cada tienda.

8. Es importante proceso de visita de tienda por parte de comprador como del asistente que la mercadería este en piso de venta así como escuchar las sugerencias de los vendedores.

Proceso de mercancías:

1. Se entrega el comprobante de crédito por la compra realizada.
2. Verifica el producto que este según el comprobante de crédito.
3. Se ingresa al sistema el detalle de la mercadería comprada.
4. Se realiza la planeación sobre la distribución de la mercancía.
5. El centro de distribución luego de realizar la planeación según las ventas mayores del producto en cada sucursal se envía el producto a las bodegas de cada tienda.
6. Inmediatamente en la bodega se ingresan los datos al sistema de las unidades en existencia en la tienda.

Procedimiento del departamento de contabilidad

1. El departamento de contabilidad posee departamentos internos importantes como lo es cuadratura que es el encargado luego de realizar las transacciones de validar las operaciones esto por medio de los auxiliares contables
2. Los auxiliares contables validan la información, en caso de existir correcciones necesitan una autorización para llevarlo a cabo.
3. Después de realizado los ajustes pertinentes, procede el departamento a registras las transacciones.

Procedimientos del departamento de sistemas

1. Realiza soportes de sistemas esto por medio de reporte de problemas de IP
2. Lleva a cabo la instalación de los equipos
3. Codifica los equipos electrónicos para un mayor control
4. Administra el sistema, así como también repara las diferencias del sistema y el funcionamiento de la maquinaria.
5. Crea los accesos a los módulos según el perfil.

Procedimientos del departamento de créditos y cobros

1. Se encarga de realizar el llenado de la solicitud de aplicación a crédito por parte los clientes se solicitan datos como salario, datos personales, referencias personales entre otros.

2. Se realiza un estudio si aplica o no al crédito otorgando tarjetas para el crédito, según sus datos así se establece el margen de crédito y las opciones del mismo.

3. Para realizar los cobros pertinentes el sistema según el tiempo que lleva sin movimientos, da aviso a proceder con los cobros de manera telefónica.

Procedimiento de inventarios

1. Se ingresa al sistema los productos luego el mismo realiza las métricas de los productos por cada Ítem cuando está en un rango de 20 a 100 unidades del producto no se genera orden de compra, cuando en el sistema existen entre 10 y 20 unidades se genera la orden de compra para el sistema de inventarios

2. El encargado del sistema digita las órdenes de compra y se procede a la autorización de las mismas

3. Después de autorizadas las órdenes de compra se realiza la compra.

4. Se ingresa al sistema la compra si necesita modificar por alguna diferencia en descripción del producto se pide una autorización para realizar el cambio.

LEGISLACIÓN

- **Ley de firma electrónica**
- **Ley de impuesto a las operaciones financieras**
- **Ley especial contra los delitos informáticos y conexos**
- **Ley de regulación de los servicios de información sobre el historial de crédito de las personas**
- **Código de comercio**
- **Código tributario y su reglamento**
- **Ley de impuesto sobre la renta**
- **Ley de Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios.**
- **Ley contra el lavado de dinero y activos y financiamiento al terrorismo.**

MEMORÁNDUM DE PLANEACIÓN

DE AUDITORÍA INTERNA AL DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN DE LA EMPRESA ALMACENES, SI VAN, S.A. DE C.V.

PERIODO DEL 01 DE ENERO AL 31 DE DICIEMBRE DE 2016

OBJETIVOS DE LA AUDITORÍA

OBJETIVO GENERAL:

Realizar una auditoría interna que evalúe las áreas de tecnologías de información hardware, software, seguridad física, seguridad lógica, data, redes y telecomunicaciones que son utilizados por la entidad para llevar a cabo sus actividades cotidianas, determinando el riesgo que posee el sistema utilizado por cada área del negocio.

OBJETIVOS ESPECÍFICOS:

- Evaluar la estructura y entorno de control interno de la entidad.
- Recopilar información sobre la realización de actividades desarrolladas en el área de Tecnologías de Información de una empresa del sector comercio evaluando el control interno de las mismas.
- Determinar los riesgos del sistema que las empresas electrodomésticas utilizan.
- Redactar programas que cumplan con los lineamientos establecidos en la normativa técnica aplicable para la realización de evaluaciones de cumplimiento por parte de auditoría interna al área de Tecnologías de Información.

ALCANCE.

Se efectuará la Auditoría Interna de acuerdo con Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna, COBIT 5 y COSO las cuales requieren que se planee y se ejecute la auditoría de tal forma que se pueda obtener una seguridad razonable de que los procesos que realiza el área de tecnologías de la información están libres de sesgos y errores significativos. El examen incluirá aquellas áreas que representen mayor riesgo las cuales se determinaran de acuerdo a la evaluación del control interno el cual dará lugar a una matriz de riesgos, considerando los siguientes componentes como lo son Hardware, Software, Seguridad Lógica, Seguridad Física, Data, Redes, Telecomunicaciones, con el propósito de expresar conclusiones y recomendaciones sobre las vulnerabilidades que se pudieran presentar debido a la práctica insuficiente de los procedimientos y controles de Tecnologías de Información.

Este examen será con base a pruebas selectivas de la evidencia que soportan los procesos, las cifras y revelaciones de los componentes descritos en el párrafo anterior; el cual incluye una evaluación de principios basados COBIT, NIEPAI y las normas de calidad ISO 27001 y 27002.

Verificar cada una de las áreas de negocio de la entidad por medio de una evaluación de control interno, recopilando información sobre cada una de las áreas, determinando los riesgos del sistema que se utilizan.

ASIGNACIÓN DE RECURSOS PARA EL TRABAJO

El personal encargado para la realización de la auditoría interna a la entidad Almacenes Si Van, S.A. de C.V. es el siguiente:

Nombre del profesional encargado.	Cargo.	Áreas
Carmen Elena Sánchez	Auditor Encargado.	- Sistemas
Roberto Menjivar Castro	Auditor Auxiliar.	- Ventas - Contabilidad - Créditos y Cobros
María del Carmen Pérez Amaya	Auditor Auxiliar.	- Recursos Humanos - Compras - Mercancías

PRESUPUESTO DE HORAS

Actividades/Horas	Encargado	Auxiliar	Auxiliar	Total
Evaluación del Control Interno y Preparación del memorando de planeación	-	10	20	**30**
Revisión y autorización de la planificación	1	5	5	**11**
Desarrollo de la Auditoría				
- Créditos y Cobros	-	25	-	**25**
- Recursos Humanos	-	-	25	**25**
- Ventas.	-	25	-	**25**
- Sistemas.	25	-	-	**25**
- Mercancías.	-	-	20	**20**
- Contabilidad.	-	20	-	**20**
- Compras	-	-	15	**15**
Revisión de PT´S	8	30	40	**78**
Elaboración y revisión de carta a la gerencia	-	20	20	**40**
Lectura y Discusión del informe con el gobierno corporativo de la entidad.	5	4	4	**13**
Total	**39**	**139**	**149**	**327**

Evaluación del sistema de control interno de la empresa.

El cuestionario de control interno es dirigido a funcionarios y personal clave dentro de la organización.

Matriz de evaluación del Sistema de Control Interno

Cliente : Almacenes Si Van S.A. de C.V.
Auditoría : Auditoría Interna a las Tecnologías de Información
Periodo : Del 01 de Enero al 31 de Diciembre 2016

Cuestionario de Auditoría Interna al Departamento de Sistemas

Preparado por : Carmen Sánchez **Fecha :20/10/2016**
Revisado por : María Pérez **Fecha :22/10/2016**
Aprobado por : Roberto Menjivar **Fecha :24/10/2016**

Nº	Pregunta	Muy en desacuerdo	En desacuerdo	Indeciso	De acuerdo	Muy de acuerdo
1	¿Utiliza COBIT 5 para la gestión de riesgos a las tecnologías de información?	1				
2	¿Posee Certificaciones ISO relacionadas a las tecnologías de Información?	1				
3	¿El software que posee la empresa es desarrollado por el departamento?					5
4	¿Establece políticas de seguridad a la gestión de redes y seguridad de los datos?				4	
5	¿El sistema cuenta con jerarquía de contraseñas para accesar al sistema, cuentas de administrador o invitados?				4	
6	¿Posee directrices para la seguridad de la información y el sistema dirigidas a usuarios ajenos a la entidad que tienen acceso al mismo?			3		
7	¿Cuenta con lineamientos específicos para la actualización de contraseñas como número de caracteres, contraseñas que no sean únicas para todos los usuarios o que se guarden las contraseñas en los equipos?		2			
8	¿Guarda bitácora sobre fallas en el sistema para realizar las correcciones debidas posteriormente?	1				
9	En caso de ocurrir intrusiones no deseadas al sistema ¿cuenta con planes de contingencia para solventar esta situación?	1				

10	¿Han robado información a la entidad por medio de ataque Phishing?		2			
11	¿Cuenta con herramientas que ayuden a la detección de intrusos al sistema de gestión?		2			
12	¿Contiene configuración a infraestructura de las tecnologías de información como protección perimetral?			3		
13	¿Implementa medidas para la detección, prevención y actualización respecto a los parches de seguridad y control de firmas de virus para proteger los sistemas de información de un software malicioso?			3		
14	Al momento de ingreso de datos al sistema ¿Posee controles de redundancia?		2			
15	¿Cuenta con planes de contingencia en caso de caídas del sistema?		2			
16	¿La empresa tiene controles de acceso a redes?				4	
17	¿Realiza intercambio de información con partes externas?	1				
18	¿Posee control de acceso al código fuente de los programas?			3		
19	¿Controla la entrada de personas internas y externas a áreas donde se procesa o almacena información sensible?				4	
20	¿Los medios de procesamiento de la información que manejan data confidencial se ubican de manera que se restrinja el ángulo de visión para evitar que la información sea vista por personas no autorizadas?	1				
21	¿Los servicios públicos de soporte son inspeccionados regularmente?	1				
22	¿Los equipos cuentan con un dispositivo de suministro de energía ininterrumpido (UPS) para apagar o el funcionamiento continuo del equipo de soporte a las operaciones comerciales críticas?				4	
23	¿Cuenta con un generador de emergencia si se requiere que el procesamiento continué en el caso de una falla de energía prolongada?				4	
24	¿El cableado de la red está protegido contra intercepciones no autorizadas o daños?		2			
25	¿Cuenta con personal de mantenimiento autorizado para llevar a cabo las reparaciones y dar servicio al equipo?			3		
26	¿Permite a los usuarios empleados, contratistas y terceras personas el retiro de los activos fuera la institución?	1				
27	¿Posee instrucciones para el manejo de errores u otras condiciones excepcionales, las cuales podrían surgir durante la ejecución del trabajo, incluyendo las restricciones sobre el uso de las utilidades del sistema?		2			
28	¿Establece políticas formales prohibiendo el uso de software no-autorizado?			3		

29	¿Realiza revisiones regulares del software y contenido de data de los sistemas que sostienen los procesos comerciales críticos?		2			
30	¿Instala y actualiza regularmente el software para la detección o reparación de códigos maliciosos?				4	
31	¿Verifica las páginas Web para detectar códigos maliciosos?				4	
32	¿Prepara planes apropiados para la continuidad del negocio para recuperarse de ataques de códigos maliciosos?			3		
33	¿La información de respaldo posee el nivel de protección física y ambiental apropiado?			3		
34	En caso de ser información confidencial ¿las copias de respaldo están debidamente protegidas por medios de codificación?		2			
35	¿Realiza pruebas regularmente para asegurar que los medio de respaldo se puedan confiar en ellos para usarlos cuando sea necesaria en caso de emergencia?	1				
36	¿Monitorea regularmente la capacidad del proveedor del servicio de red para manejar los servicios contratados de una manera segura?	1				
37	¿Restringe el acceso a los servicios de red o aplicaciones?			3		
38	¿Posee procedimientos para proteger la información electrónica confidencial que está en la forma de un adjunto?					
39	¿Cuenta con política para el uso de comunicación inalámbrica, tomando en cuenta los riesgos particulares involucrados?		2			
40	¿Utiliza técnicas de codificación para proteger la confidencialidad, integridad y autenticidad de la información que se transmite electrónicamente?	1				
41	¿Permite el envío de información a correos externos al de la institución?				4	
42	¿Posee procedimientos para asegurar el rastreo y no repudio?			3		
43	¿Utiliza IDs de usuarios únicos para permitir a los usuarios vincularse y ser responsables de sus acciones?				4	
44	¿Mantiene un registro formal de todas las personas registradas para usar el servicio?				4	
45	¿Elimina o bloquea inmediatamente los derechos de acceso de los usuarios que han cambiado de puesto o trabajo o han dejado la organización?			3		
46	¿Se asegura que no se emitan IDs de usuario redundantes a otros usuarios?				4	
47	¿Los sistemas de cómputo permiten guardar las contraseñas de los usuarios?				4	

48	¿Posee procedimientos de autorización para determinar quién está autorizado a tener acceso a cuáles redes y servicios en red?		2			
49	¿Realiza registro de los intentos exitosos y fallidos de autenticación del sistema?	1				
50	¿El sistema limita el número de intentos de registro infructuosos permitidos?				4	
51	¿Posee numeración en los equipos?					5
52	¿El sistema cuenta con un control de acceso restringido a información confidencial?		2			
53	¿Existen procedimientos diseñados para proteger el intercambio de información de la intercepción, copiado, modificación, routing equivocado y destrucción de la misma?			3		
54	¿Cuentan con políticas o lineamientos señalando el uso aceptable de los medios de comunicación electrónicos para evitar pérdidas o robo de información confidencial?			3		
	Total	**12**	**24**	**39**	**56**	**10**

Riesgo Alto desde 54 a 162 puntos
Riesgo Medio desde 162 a 216 puntos
Riesgo bajo desde 216 a 270 puntos

Tipo de Riesgo **Alto**
Total puntaje **141**

Cliente : Almacenes Si Van S.A. de C.V.
Auditoría : Auditoría Interna a las Tecnologías de Información
Periodo : Del 01 de Enero al 31 de Diciembre 2016

Cuestionario de Auditoría Interna al Departamento de Créditos y Cobros

Preparado por : Carmen Sánchez **Fecha: 20/10/2016**
Revisado por : María Pérez **Fecha: 22/10/2016**
Aprobado por : Roberto Menjivar **Fecha: 24/10/2016**

Nº	Pregunta	Muy en desacuerdo	Desacuerdo	Indeciso	De acuerdo	Muy de acuerdo
1	¿Cuenta con un sistema para registro de los datos de los clientes?					5
2	¿El acceso a este sistema es jerarquizado?				4	
3	¿Permite realizar cambios a los datos de los clientes a los usuarios del sistema?				4	
4	¿El sistema permite extraer información de los clientes para uso de otros departamentos?		2			
5	¿El sistema de créditos se encuentra vinculado con otros departamentos?				4	
6	¿El sistema de cobros posee alertas sobre los créditos vencidos?	1				
7	¿Los cobros realizados por los clientes se ingresan al sistema de manera manual?			3		
8	¿Los usuarios modifican los datos pertinentes a los cobros de los clientes?			3		
9	Al cancelar una de las cuentas de los clientes ¿Los datos pertinentes son actualizados al sistema de los demás departamentos a los que está vinculado?			3		
10	¿La información que está dentro del sistema se encuentra encriptada?	1				
11	¿El sistema cuenta con firma digital al momento de realizar transacciones los usuarios?		2			
12	¿Conserva una bitácora de los usuarios que ingresan al sistema de créditos y cobros así como también las operaciones que realiza dentro de él?	1				
13	¿Los usuarios poseen restricción al uso de todas las funciones del sistema?				4	
14	¿La información que está en el sistema cuenta con su respectivo respaldo?			3		

15	¿El sistema permite el ingreso de redundancias al momento de ingresar los números de clientes?	1				
16	¿La transmisión de los datos lo realiza por medio de la red?			3		
17	¿Posee restricción de acceso a la Red?			3		
18	¿Segrega las tareas de ingreso de datos al sistema?			3		
19	¿Cuenta con manuales de procedimientos sobre las actividades del departamento?				4	
20	¿Realiza revisiones periódicas a las políticas de seguridad informática?		2			
21	¿Está consciente de las vulnerabilidades que posee el sistema?		2			
22	¿Transmite información confidencial por medios electrónicos?			3		
23	¿Las transacciones realizadas por medio de cuentas bancarias por pago de cuentas de los clientes esta vinculadas al módulo de créditos y cobros?	1				
24	¿Cuenta con procedimientos para cerrar cuentas de clientes?	1				
25	¿Posee restricción para realizar modificaciones cuando se ha cerrado un número de usuario?			3		
26	Al momento de la cancelación de una deuda ¿El sistema cierra la cuenta del cliente automáticamente?	1				
27	¿Usuarios externos tienen acceso a información del sistema?				4	
28	¿Cuenta con planes de contingencia en caso de fallar el sistema?			3		
29	¿Realiza un control sobre fallas en el sistema?	1				
30	¿Cuenta con soporte y mantenimiento al sistema?				4	
		8	8	30	28	5

Riesgo Alto desde 30 a 90 puntos
Riesgo Medio desde 90 a 120 puntos
Riesgo bajo desde 120 a 150 puntos

Tipo de Riesgo **Alto**
Total puntaje **79**

Cliente : Almacenes Si Van S.A. de C.V.
Auditoría : Auditoría Interna a las Tecnologías de Información
Periodo : Del 01 de Enero al 31 de Diciembre 2016

Cuestionario de Auditoría Interna al Departamento de Mercancía

Preparado por : Carmen Sánchez **Fecha: 20/10/2016**
Revisado por : María Pérez **Fecha: 22/10/2016**
Aprobado por : Roberto Menjivar **Fecha: 24/10/2016**

Nº	Pregunta	Muy en desacuerdo	Desacuerdo	Indeciso	De acuerdo	Muy de acuerdo
1	¿El sistema de Mercancías se encuentra vinculado con el sistema de bodega principal y las bodegas de cada sucursal?			3		
2	¿Cuándo se ingresan las órdenes de compras al sistema lleva correlativo de las mismas?				4	
3	Al ingreso de las órdenes de compra ¿Guarda registro de los usuarios que realizan dicha acción?				4	
4	¿El sistema de mercancías permite modificaciones a las órdenes de compras?				4	
5	¿Controla el manejo de los inventarios por medio de un sistema?					5
6	¿El sistema de este departamento está en red?				4	
7	Cuándo surgen cambios en la organización que afecten al sistema de mercancías ¿Se realizan las actualizaciones al sistema inmediatamente?		2			
8	¿El sistema de mercancías se encuentra protegido contra alteraciones y accesos no deseados?				4	
9	¿Los datos de los inventarios son ingresados al sistema de manera manual?				4	
10	¿El registro de las operaciones dentro del sistema se encuentra debidamente respaldadas con back-up?				4	

11	¿Realiza pruebas para comprobar el buen funcionamiento de esos respaldos?		2			
12	¿Aísla los ítems que requieren protección especial para reducir el nivel general de la protección requerida?	1				
13	¿Los datos del sistema se comparan con las existencias físicas?		2			
14	¿El sistema genera reportes de los inventarios?				4	
15	¿El sistema posee unos ítems que refleje los productos más vendidos?				4	
16	¿El modulo del departamento se encuentra vinculado a las demás áreas de negocio?			3		
17	¿El sistema se encuentra jerarquizado?			3		
18	¿Permite realizar modificaciones en el sistema por parte de cualquier usuario?	1				
19	¿Se realizan mantenimientos periódicos al sistema?			3		
20	¿Existe seguridad perimetral para el resguardo de las mercancías y equipo informático?		2			
		2	8	12	36	5

Riesgo Alto desde 20 a 60 puntos
Riesgo Medio desde 60 a 80 puntos
Riesgo bajo desde 80 a 100 puntos

Tipo de Riesgo **Medio**
Total puntaje **63**

Cliente : Almacenes Si Van S.A. de C.V.
Auditoría : Auditoría Interna a las Tecnologías de Información
Periodo : Del 01 de Enero al 31 de Diciembre 2016

Cuestionario de Auditoría Interna al Departamento de Ventas

Preparado por : Carmen Sánchez **Fecha: 20/10/2016**
Revisado por : María Pérez **Fecha: 22/10/2016**
Aprobado por : Roberto Menjivar **Fecha: 24/10/2016**

Nº	Pregunta	Muy en desacuerdo	Desacuerdo	Indeciso	De acuerdo	Muy de acuerdo
1	¿Poseen un sistema de control de ventas?					5
2	¿Frecuentemente se actualiza dicho sistema?				4	
3	¿El sistema permite realizar ventas al crédito por vía electrónica?		2			
4	¿El sistema cuenta con instrucciones para el manejo de errores u otras condiciones excepcionales, las cuales podrían surgir durante la ejecución de la transacción?			3		
5	¿Considera que al momento de otorga créditos electrónicos el sistema se encuentra capacitado para verificar los datos pertinentes para otorga el crédito?		2			
6	¿El sistema permite generar reportes acerca de las ventas realizadas en el día?				4	
7	Al momento de realizar un pedido o generar una venta ¿Existen controles de seguridad que restringen el acceso sólo al personal autorizado?			3		
8	¿El sistema de venta presenta las fechas y horas en que son realizadas las ventas?				4	
9	¿El sistema emite reportes de las ventas realizadas con CCF y Facturas?			3		
10	¿Existen campos obligatorios en el sistema de facturación?				4	
11	¿Cuentan con procedimientos de emergencia y respaldo para resguardar la información contenida en el sistema?				4	
12	¿Es visible para los usuarios del sistema los acuerdos de seguridad que posee, definiciones del sistema y aspectos de la gestión del mismo?			3		

13	¿El sistema de facturación cuenta con instrucciones para el manejo de output especiales y medios, tales como el uso de papelería especial o el manejo de output confidencial incluyendo los procedimientos para la eliminación segura de documentos de facturación?				4	
14	¿Al momento de cambios de sistemas de facturación realizan una evaluación de los impactos potenciales de los cambios, incluyendo los impactos de seguridad?		2			
15	¿Cuándo existen cambios en los sistemas de facturación efectúan capacitaciones al personal?		2			
16	¿Se realizan evaluaciones para monitorear y revisar las condiciones de seguridad de los sistemas?		2			
17	¿El sistema proporciona información sobre incidentes de seguridad de la información y la revisión de esta información por terceros?		2			
18	¿Poseen controles de detección, prevención y recuperación para proteger el sistema contra códigos maliciosos?			3		
19	¿Los controles de detección de amenazas son los más adecuados?		2			
20	¿Se implementan procedimientos para que los usuarios del sistema tengan los apropiados conocimientos de los controles de detección, prevención y recuperación contra códigos maliciosos?			3		
21	¿Existen políticas formales prohibiendo el uso de software no-autorizado que pueden dañar el sistema?		2			
22	¿Los servidores donde se maneja el sistema cuentan con instalación y actualización regular de software para la detección o reparación de códigos maliciosos?			3		
23	¿Los respaldos que se realizan se encuentran almacenados en un lugar apartado, con una distancia suficiente para escapar de cualquier daño por un desastre en el local principal?			3		
24	¿Los respaldos de información confidencial de los clientes cuentan con una codificación para evitar que cualquier usuario tenga acceso a ella?				4	
25	¿Se cuenta con procedimientos para el manejo y almacenaje de información para proteger esta información de una divulgación no-autorizada o mal uso?			3		
26	¿El sistema genera un reporte sobre las ventas realizadas en efectivo y con tarjeta?			3		
		0	16	30	28	5

Riesgo Alto desde 26 a 60 puntos
Riesgo Medio desde 60 a 80 puntos
Riesgo bajo desde 80 a 100 puntos

Tipo de Riesgo **Medio**
Total puntaje **79**

Cliente : Almacenes Si Van S.A. de C.V.
Auditoría : Auditoría Interna a las Tecnologías de Información
Periodo : Del 01 de Enero al 31 de Diciembre 2016

Cuestionario de Auditoría Interna al Departamento de Contabilidad

Preparado por : Carmen Sánchez **Fecha: 20/10/2016**
Revisado por : María Pérez **Fecha: 22/10/2016**
Aprobado por : Roberto Menjivar **Fecha: 24/10/2016**

Nº	Pregunta	Muy en desacuerdo	Desacuerdo	Indeciso	De acuerdo	Muy de acuerdo
1	¿Cuentan con un sistema que genere los reportes contables necesarios?				4	
2	¿El sistema que utiliza el departamento genera back-up?				4	
3	¿Se instalan todas las actualizaciones sugeridas por el proveedor del sistema?		2			
4	¿Se realizan actualizaciones constantes al sistema contable?			3		
5	¿El sistema se encuentra jerarquizado?			3		
6	¿El sistema brinda reporte de conciliaciones de saldos?				4	
7	¿El sistema detecta redundancias en las partidas contables?		2			
8	¿El sistema cuenta con un manual para los usuarios?			3		
9	¿Es compatible el sistema con cualquier sistema operativo?		2			
10	¿Se cuenta con una licencia de uso del sistema contable?				4	
11	¿El sistema permite el control sobre la cuadratura de las partidas contables?		2			
12	¿El sistema cuenta con la función de totalizar las partidas?				4	
13	¿Se puede importar y exportar datos de otros programas al sistema contable?		2			
14	¿El módulo de contabilidad se encuentra vinculado a los módulos de otros departamentos?			3		
15	¿Permite el sistema realizar cambios a estados financieros de periodos anteriores?				4	
			10	12	24	0

Riesgo Alto desde 15 a 45 puntos
Riesgo Medio desde 45 a 60 puntos
Riesgo bajo desde 60 a 75 puntos

Tipo de Riesgo **Medio**
Total puntaje **46**

Cliente : Almacenes Si Van S.A. de C.V.
Auditoría : Auditoría Interna a las Tecnologías de Información
Periodo : Del 01 de Enero al 31 de Diciembre 2016

Cuestionario de Auditoría Interna al Departamento de RRHH

Preparado por : **Carmen Sánchez** **Fecha: 20/10/2016**
Revisado por : **María Pérez** **Fecha: 22/10/2016**
Aprobado por : **Roberto Menjivar** **Fecha: 24/10/2016**

Nº	Pregunta	Muy en desacuerdo	Desacuerdo	Indeciso	De acuerdo	Muy de acuerdo
1	¿Los acuerdos contractuales con empleados o contratistas indican sus responsabilidades en cuanto a seguridad de la información?				4	
2	¿Se posee disponibilidad de referencias tanto personales como comerciales de los postulantes a emplear?				4	
3	¿Se efectúan chequeos de récords criminales de los postulantes a emplear?			3		
4	¿Los empleados deben de firmar un acuerdo de confidencialidad o no divulgación antes de otorgarles acceso a los medios de procesamiento de la información?			3		
5	¿Se revisa constantemente los requisitos de confidencialidad o acuerdos de no divulgación que proteja la información de la organización?		2			
6	¿El personal posee las habilidades en TI suficientes para las competencias requeridas para su función?		2			
7	¿Se debe tener un proceso de inducción formal diseñado para introducir políticas y expectativas de seguridad de la organización antes de otorgar acceso a la información a los empleados?	1				
8	¿Las capacitaciones deben incluir requerimientos de seguridad, responsabilidades legales y controles comerciales, así como uso correcto de los medios de procesamiento de la información?		2			
9	¿Se posee información documentada adecuada como evidencia de las competencias de los empleados?		2			
10	¿La gerencia debe informar apropiadamente a los empleados sobre sus roles y responsabilidades de seguridad antes de otorgarles acceso a información confidencial o a los sistemas de información?				4	
11	¿Las personas que laboran para la empresa conocen la política de seguridad de la información de esta?				4	

12	¿Los empleados tienen que conocer la responsabilidad con relación al manejo de la información recibida de otras compañías?			3		
13	¿Los empleados contribuyen a la eficacia del sistema de gestión de la seguridad de la información?		2			
14	¿Existe un proceso disciplinario formal para empleados que hayan cometido una infracción a la seguridad de la información?					5
15	¿El proceso disciplinario debería proporcionar una respuesta equilibrada que tome en consideración factores como la naturaleza y gravedad del incumplimiento y su impacto en el negocio?					5
16	¿En casos serios de dolo, el proceso disciplinario debería permitir la remoción inmediata del empleado y de los derechos de acceso y privilegios de este?					5
17	¿Se definen contractualmente las responsabilidades de las personas respecto a la seguridad de la información después de una desvinculación laboral?				4	
18	¿Los empleados deben devolver todos los activos de la organización que tengan en su posesión a término de su vínculo laboral?	-			4	
19	¿En caso que el empleado utilice su propio equipo, se debieran seguir procedimientos para asegurar que toda información relevante sea transferida a la organización y sea borrada adecuadamente del equipo?				4	
20	¿Los derechos de acceso de todos los empleados a la información y los medios de procesamiento de información son retirados a la terminación de su empleo?				4	
21	¿Los derechos de acceso que se deben retirar incluyen el acceso físico y lógico, llaves, tarjetas de identificación, medio de procesamiento de la información, suscripciones y el retiro de cualquier documentación que identifique a la persona como miembro actual de la organización?				4	
22	¿Si un empleado conoce claves secretas de cuentas activas se efectúan cambios de claves a la terminación de la vinculación laboral?					5
23	¿Los derechos de acceso a la información se retiran antes de la terminación del empleo si el proceso de despido lo ha iniciado la gerencia?			3		
24	¿En casos en los que la gerencia inicia las terminaciones laborales se poseen procedimientos para evitar que los empleados corrompan la información deliberadamente o saboteen los medios de procesamiento de la información?					5
		1	10	12	36	25

Riesgo Alto desde 24 a 72 puntos
Riesgo Medio desde 72 a 96 puntos
Riesgo Bajo desde 96 a 120 puntos

Tipo de riesgo Medio
Total Puntaje 84

Cliente : Almacenes Si Van S.A. de C.V.
Auditoría : Auditoría Interna a las Tecnologías de Información
Periodo : Del 01 de Enero al 31 de Diciembre 2016

Cuestionario de Auditoría Interna al Departamento de Compras

Preparado por : Carmen Sánchez **Fecha: 20/10/2016**
Revisado por : María Pérez **Fecha: 22/10/2016**
Aprobado por : Roberto Menjivar **Fecha: 24/10/2016**

Nº	Pregunta	Muy en desacuerdo	Desacuerdo	Indeciso	De acuerdo	Muy de acuerdo
1	¿Se posee un resguardo sobre las órdenes de compra emitidas, para cotejarla con la factura correspondiente?				4	
2	¿Se cuenta con firmas electrónicas al momento de hacer depósitos a proveedores para dar autenticidad al pago?		2			
3	¿Poseen respaldo los pagos que se efectúan vía electrónica?				4	
4	¿Se posee un sistema que controle las compras realizadas por la empresa?					5
5	¿El sistema de compras posee una opción para hacer los ingresos de los productos al inventario de bodega?				4	
6	¿Se efectúan revisiones de mantenimiento al equipo utilizado por el departamento de compras?			3		
7	¿Los empleados del departamento de compras poseen acceso total al sistema de la empresa, o solo al sistema de compras?				4	
8	¿El sistema de compras está vinculado a contabilidad para la realización de partidas contables automáticas?		2			
9	¿Los encargados de compras conocen los procedimientos para la seguridad de la información?				4	
10	¿Los equipos informáticos del departamento de compras poseen acceso total a internet o solo a páginas web necesarias para los procesos realizados en este?		2			
11	¿Los enunciados de los requerimientos comerciales para los sistemas de información nuevos especifican los requerimientos de los controles de seguridad?				4	

12	¿Los controles de seguridad reflejan el daño comercial potencial que podría resultar de una falla o ausencia de seguridad?				4	
13	Si los productos son comprados y no desarrollados por la entidad ¿Se realizan un proceso de prueba y adquisición formal?	1				
14	¿Los contratos con los proveedores tratan los requerimientos de seguridad identificados?			3		
15	Cuando la funcionalidad de la seguridad de un producto propuesto no satisface el requerimiento especificado ¿Se reconsideran el riesgo y los controles asociados antes de comprar el producto?				4	
		1	6	6	32	5

Riesgo Alto desde 15 a 45 puntos
Riesgo Medio desde 45 a 60 puntos
Riesgo Bajo desde 60 a 75 puntos

Tipo de riesgo	Medio
Total puntaje	50

MATRIZ DE RIESGO								
PROCEDIMIENTO	**FACTOR DEL RIESGO**	**DESCRIPCIÓN DEL RIESGO**	**CALIFICACIÓN**			**CLASIFICACIÓN**		
			PR	I	ER	B	M	A
a) CRÉDITOS Y COBROS								
	El sistema no realiza avisos sobre cuentas vencidas	El ingreso por cuenta de los clientes que no han efectuado los pago en las fechas correspondientes no dejan de ser percibidos por la empresa	3	3	9			ALTO
b) RECURSOS HUMANOS								
	Firma por parte de los empleados de un acuerdo de confidencialidad antes de otorgarles acceso a los medios de procesamiento de la información.	El robo de información por parte de un empleado y que este no pueda ser condenado por no haber un documento que respalde la confidencialidad de la información manejada por la empresa.	2	3	6			ALTO
c) VENTAS								
	Falta de controles en acceso y manipulación de información, falta de evaluación de impactos en cambios de sistemas	Extravió o mal uso de información confidencial y vital para la empresa, pérdida irreparable de información y fallas en los servicios.	2	3	6			ALTO
d) SISTEMAS								
	Caídas en el sistema que utiliza la entidad ya que no se cuenta con planes de contingencia en caso de ocurrencia	Que el trabajo de todos los departamentos se vea afectado ya que estos están en vinculados entre sí.	2	3	6			ALTO

e)	**MERCADERÍA**					
	Permite realizar cambios a la información que se posee en el sistema sin restricción	Que se realice perdidas de mercaderías de las bodegas de la empresa	2	2	4	MEDIO
f)	**CONTABILIDAD**					
	Falta de actualizaciones recomendadas, incompatibilidad con sistemas operativos e importación y exportación de datos.	Fallas en el sistema, perdida de información. Limita obtener información en formatos manipulables para toma de decisiones y adaptabilidad a diferentes equipos.	2	2	4	MEDIO
g)	**COMPRAS**					
	Los empleados del departamento de compras conocen los procedimientos para la seguridad de la información.	Por desconocimiento los encargados de compras realicen acciones que afecten la seguridad de la información en sus quehaceres laborales	1	2	2	BAJO

Identificación de Áreas Críticas

Dentro del proceso de auditoría se identificaron las principales áreas críticas que se deben considerar para su ejecución las cuales son:

ALTO

a) Créditos y Cobros.
b) Recursos Humanos.
c) Ventas.
d) Sistemas.

Al realizar la evaluación de control interno el área más expuesta al riesgo se encuentra el área de créditos y cobros, debido a que se encuentra expuesta a muchos factores de riesgo, al otorgar créditos en ventas realizadas electrónicamente, así como en las diferentes sucursales, siendo una de las principales fuentes de ingresos para la entidad dichas ventas al crédito, es por ello que es el área a la que más se debe evaluar para medir su riesgo.

Otra de las áreas que posee un alto riesgo es recursos humanos, debido a que el personal está más vulnerable a cometer errores al momento de ingresar los datos al sistema así como también por conductas inadecuadas al momento de manipular datos de clientes; además se encuentran ubicadas en niveles de riesgo alto el área de ventas y sistemas.

MEDIO

a) Mercadería
b) Contabilidad

El departamento de mercancías y contabilidad son otras áreas que se ven expuestas a un riesgo medio, el cual puede representar un impacto no de gravedad para la empresa pero que debe tomarse en cuenta a fin de poder prevenir incidentes de mayor gravedad para la entidad

BAJO

c) Compras

El departamento de compras es el que se encuentra expuesto a un riesgo bajo, no representando un área critica dentro de la entidad, sin embargo se debe evaluar para prevenir posibles riesgos que pudieran ser perjudiciales para el desarrollo efectivo de la actividad económica.

4.2.2 PROGRAMAS DE AUDITORÍA

Cliente : Almacenes Si Van S.A. de C.V.
Auditoría: Auditoría Interna a las Tecnologías de Información
Periodo : Del 01 de Enero al 31 de Diciembre 2016

Programa de Auditoría Interna con Base a Buenas Prácticas

Preparado por : **Fecha :**
Revisado por : **Fecha :**
Aprobado por : **Fecha :**

A. Área: Créditos y Cobros

N°	Naturaleza o alcance de los procedimientos de auditoría	Ref. Pts.	Elaborado por
1	Verifique que la funcionalidad del software de aplicación adquirido cumpla con los siguientes aspectos: 1) Elaboración de informes crediticios, 2) Cálculo de impuestos de acuerdo a legislación aplicable 3) Tazas de interés, 4) Alertas sobre cuentas de clientes sin pagar.		
2	Revise si se tienen establecidos los criterios de aceptación para: 1) los sistemas de información nuevos, 2) actualizaciones 3) Para llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación.		
3	Corrobore si el sistema cuenta con cierre automático de sesiones inactivas y elabore una narrativa detallando el proceso de cierre de sesión.		
	Verifique si se cuenta con políticas para: 1)almacenamiento de los datos 2) localización 3) capacidad de recuperación.		
4	Compruebe que se realizan back-ups por medios electrónicos y desarrolle una narrativa que exprese que estos sean probados regularmente.		
5	Verifique que se protege el acceso de la información disponible públicamente para evitar la modificación no autorizada, realizando una narrativa que documente las medidas de seguridad que utiliza.		
6	Inspeccione si se poseen especificaciones para: 1) documentar las entradas de datos (independientemente de la fuente) 2) validaciones para las transacciones del departamento 3) los métodos de validación de datos.		

N°	Naturaleza o alcance de los procedimientos de auditoría	Ref. Pts.	Elaborado por
7	Verifique a través de documentos oficiales emitidos por la gerencia si se cuenta con políticas para proteger la información involucrada en el comercio electrónico de cualquier actividad fraudulenta.		
8	Observe si la entidad implementa mecanismos para garantizar que la información sea clara, precisa y que pueda ser verificable.		
9	Corroboré con el encargado del departamento que dentro del manual de políticas se establecen lineamientos dirigidos a la integridad de la información disponible públicamente para evitar la modificación no autorizada.		
10	Inspeccione si en los contratos se han establecido acuerdos para el intercambio de información entre la organización y entidades externas.		
11	Elabore una cédula que detalle los periodos en que se realizaron evaluaciones a los mecanismos de intercambio de información con interesados externos e internos.		
12	Realice un muestreo con el personal del departamento para identificar los roles que se han establecido en el uso del sistema de información, luego prepare una narrativa que exprese los roles y las responsabilidades del mismo		
13	Verifique si el sistema permite extraer información de los clientes para uso de otros departamentos		
14	Inspeccione si antes de otorgar acceso a la información se evalúa si cumple con los requerimientos de seguridad siguientes: 1) si está protegida por corta fuegos 2) los datos están encriptados 3) utiliza claves para tener acceso a la información.		
15	Verifique que los documentos dentro del sistema están sujetos a responsabilidades por medio de firma electrónica.		
16	Inspeccione si se cuenta con prácticas de supervisión para garantizar que los roles y las responsabilidades se ponga en práctica de forma correcta dentro del sistema, mediante una narrativa exprese las prácticas utilizadas		
17	Verifique por medio de bitácora del sistema si se registran las actividades del administrador y operador del sistema		
18	Verifique si el departamento cuenta con políticas para conducir las expectativas de control de TI en temas relevantes, como calidad, seguridad, confidencialidad, controles internos, uso de activos de TI, ética y derechos de propiedad intelectual dentro del departamento mediante narrativa documente dichas políticas.		

N°	Naturaleza o alcance de los procedimientos de auditoría	Ref. Pts.	Elaborado por
19	Indague con el encargado del departamento si el manual de políticas está aprobado por los gerentes para asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad, elabore una narrativa que documente el acuerdo de aprobación del manual de políticas por parte de la gerencia y anexe el manual de políticas.		
20	Indague con la gerencia si realiza actualizaciones a las políticas, como minino una vez al año, para ajustarlas a los cambiantes entornos operativos o de negocio; mediante narrativa exprese los periodos en que se realizaron las actualizaciones anexe los cambios que se realizaron.		
21	Indague con el personal del departamento si la entidad se encuentra consiente de las debilidades del diseño (por ejemplo, inconsistencias, fallas de claridad) identificando mejoras cuando se requieran, mediante narrativa detalle las debilidades expresadas por el personal.		
22	Verifique si el sistema cuenta con procesos de liquidación automático de cuentas de clientes para evitar impactos negativos que afecten la efectividad del sistema elabore una narrativa que detalle el proceso de cierre de cuentas de clientes.		
23	Verifique si se cuenta con registros sobre eventos de riesgo que han causado o pueden causar impactos al beneficio facilitado por TI, a la entrega de programas y proyectos de TI, mediante narrativa capturar datos relevantes sobre asuntos relacionados, incidentes, problemas e investigaciones.		
24	Verifique si se han corregido las fallas registradas en el sistema y mediante narrativa exprese las fallas y las correcciones realizadas.		
25	Verifique si se cuenta con políticas para preparar, mantener y probar planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente con un impacto de negocio grave, realice una narrativa detallando las principales políticas con que se cuentan.		
26	Inspeccione si se realizan mantenimientos periódicos al equipo tecnológico del departamento para permitir su continua disponibilidad realice cédula de detalle que muestre las fechas en que se llevó a cabo el mantenimiento de los equipos en el año y las actividades que se realizaron anexando la documentación que respalde dicho mantenimiento.		
27	Verifique si se cuenta con lineamientos para proteger la información involucrada en las transacciones en línea para evitar la transmisión incompleta, rutas equivocadas, alteración no-autorizada del mensaje, divulgación no-autorizada, y duplicación o re-envío no autorizado del mensaje, al momento de realizar los pagos los clientes y mediante una narrativa documente los lineamientos.		
28	Indague si se cuenta con políticas para segregar los deberes y áreas de responsabilidad para reducir las amenazas de modificación no-autorizada o no-intencionada o un mal uso de los activos de la organización documente mediante narrativa las políticas empleadas.		

Cliente : Almacenes Si Van S.A. de C.V.
Auditoría : Auditoría Interna a las Tecnologías de Información
Periodo : Del 01 de Enero al 31 de Diciembre 2016

Programa de Auditoría Interna con Base a Buenas Prácticas

Preparado por : **Fecha :**
Revisado por : **Fecha :**
Aprobado por : **Fecha :**

A. Área:	**Recursos Humanos**

N°	**Naturaleza o alcance de los procedimientos de auditoría**	**Ref. Pts.**	**Elaborado por**
1	Inspeccione los equipos informáticos del departamento de recursos humanos y efectué una cédula narrativa detallando si los software instalados poseen licencias de uso vigentes.		
2	Solicite la lista de activo fijo de los equipos utilizados en el departamento de recursos humanos, efectué una inspección revisando que cada equipo posea su respectivo código y cotéjelo con la lista proporcionada.		
3	Desarrolle una cédula narrativa mencionando los controles que se poseen para el resguardo del activo fijo del departamento de recursos humanos.		
4	Verifique que cada equipo informático del departamento de recursos humanos posea adecuados reguladores de voltaje y que estos tengan la capacidad suficiente para la protección de cada equipo, dejando constancia en una narrativa de lo observado en dicha verificación.		
5	Indague si la entidad posee un manual donde se explique cada rol a desempeñar por parte de los empleados y su responsabilidad respecto a la seguridad de la información, elabore una narrativa dejando evidencia de lo realizado.		
6	Elabore narrativa en la cual se describa si los empleados de la entidad al comenzar el empleo en la organización recibieron instrucciones respecto a sus roles y la responsabilidad que estos tendrían respecto a la seguridad de la información.		
7	Desarrolle narrativa en la cual se indague si la empresa posee procedimientos establecidos para controlar la divulgación de información confidencial.		
8	Inspección si la entidad posea un proceso disciplinario formal el cual castigue a empleados que han cometido infracciones entorno a la seguridad de la información, elabore una narrativa en el cual desarrolle los procesos sancionatorios para todas las infracciones detalladas en el documento.		

N°	Naturaleza o alcance de los procedimientos de auditoría	Ref. Pts.	Elaborado por
9	Indague con empleados si estos poseen conocimiento sobre la existencia de un proceso disciplinario que castigue por infracciones cometidas a la seguridad de la información, desarrolle una narrativa con los comentarios proporcionados por los empleados.		
10	Indague si se han suscitado acontecimientos referidos a la seguridad de la información, y desarrolle una narrativa en la cual se detallen las formas en cómo ha sido sancionada tal acción, para determinar si se aplica o no el proceso disciplinario que la entidad posee.		
11	Indague el procedimiento para la recuperación de información almacenada en equipos que sean propiedad del empleado que termina su vínculo laboral con la entidad y desarrolle una narrativa mencionando las ventajas y desventajas de dicho proceso.		
12	Indague la existencia de un procedimiento para el retiro de accesos a la información que los empleados utilizan durante el vínculo laboral con la entidad y elabore una narrativa de lo investigado.		
13	Indague sobre la existencia de un procedimiento para el cambio de claves secretas que sean de conocimiento de algún empleado que ha dejado de ser parte de la entidad y desarrolle una narrativa en la cual se expliquen los procesos plasmados en el documento y si son aplicados correctamente en caso de ser necesarios.		
14	Realice una inspección para verificar si el sistema utilizado por el departamento de recursos humanos esta jerarquizado y explique en una narrativa como es el proceso para la creación de nuevos usuarios para dicho sistema.		
15	Instale un programa en un equipo del departamento de recursos humanos y observe las alertas y restricciones que el sistema emplea para evitar la instalación de programas ajenos a los utilizados por la entidad.		
16	Indague si la empresa posee procedimientos para la recuperación de activos que hayan sido utilizados por los ex empleados durante su vínculo laboral con la entidad y elabore una narrativa exponiendo los controles utilizados para las situaciones antes mencionadas.		
17	Elabore una narrativa explicando los procedimientos que la empresa emplea para evitar que los empleados saboteen o corrompan deliberadamente los medios de procesamiento de la información.		
18	Inspeccione los procesos de contratación que se efectúan en la entidad y elabore una narrativa expresando si duchos procesos están acorde a las políticas establecidas por la organización.		
19	Revise los contratos de los empleados de la empresa y verifique si se establezcan en ellos las responsabilidades respecto a la seguridad de la información.		

N°	Naturaleza o alcance de los procedimientos de auditoría	Ref. Pts.	Elaborado por
20	Indague con un encargado del departamento de recursos humanos si poseen un archivo de referencias de récords criminales de los empleados de la entidad.		
21	Solicite cada uno de los archivos de postulantes que tenga la empresa, elabore una narrativa explicando si se solicita referencias personales o de empleos pasados.		
22	Verifique si la empresa emplea controles en el proceso de contratación de empleados para el área de TI y elabore una narrativa en la cual se expongan las características que el postulante debe poseer para optar al cargo.		
23	Indague si existe un documento de acuerdo de confidencialidad que proteja la información de la entidad, solicite una fotocopia para poder revisarlo detenidamente y emitir recomendaciones respecto a dicho documento.		
24	Verifique las clausulas contenidas en el acuerdo de confidencialidad observando que estás estén con base en leyes aplicables y políticas establecidas por la empresa para la divulgación de la información		
25	Verifique que cada empleado haya hecho efectiva su firma sobre el documento de confidencialidad que resguarda la información de la empresa.		
26	Indague con un encargado del departamento de recursos humanos si los acuerdos de confidencialidad son revisados constantemente y elabore una narrativa en la cual se explique si estos son actualizados respecto a nuevas necesidades existentes en la entidad para el óptimo resguardo de la información.		
27	Indague si la entidad posee un documento donde se muestre el perfil de la persona a contratar y desarrolle una narrativa en la que se exponga si dicho documento muestra las características necesarias para la función que desempeñará el postulante.		
28	Inspeccione si la entidad realiza evaluaciones a sus empleados para constatar los conocimientos de estos y elabore una narrativa comentando el proceso empleado por la empresa para la realización de las evaluaciones a los empleados.		
29	Indague con personal de la empresa si esta les proporciona a los nuevos empleados un manual donde se expliquen las funciones que desempeñara en su puesto de trabajo.		
30	Observe el contenido de las capacitaciones recibidas por los empleados, dejando constancia en una narrativa si se les imparten los conocimientos necesarios para las funciones que desempeñan en la entidad.		
31	Verifique la constante actualización del contenido de las capacitaciones a empleados, para que éstos estén a la vanguardia de las funciones que desempeñan en la organización.		

N°	Naturaleza o alcance de los procedimientos de auditoría	Ref. Pts.	Elaborado por
32	Solicite al encargado del departamento de recursos humanos un documento que evidencie las capacitaciones a las que han asistido los empleados con el objeto de comprobar la realización de capacitaciones.		
33	Observe los procedimientos utilizados respecto a la recepción de información proveniente de otras entidades y elabore una narrativa explicando el proceso y emitiendo conclusiones de éste.		
34	Indague si los empleados logran las metas establecidas por la entidad, ya que ello conlleva la conquista de los objetivos trazados por la organización elabore una narrativa detallando si los empleados reciben algún tipo de compensación por el logro de metas.		
35	Verifique la aplicación del código de ética que rige las acciones de sus empleados, elabore una narrativa sobre el contenido del código de ética utilizado y si es correcta la aplicación de este en la entidad.		
36	Observe el proceso disciplinario aplicado por la entidad, elabore una narrativa explicando si se emplean los criterios necesarios y actualizados para sancionar las infracciones cometidas a la seguridad de la información.		
37	Elabore una narrativa exponiendo si en los contratos se definen las responsabilidades por parte de los empleados al término de su vínculo laboral con la empresa.		
38	Indague si la entidad posee procedimientos para evitar que los empleados saboteen o corrompan deliberadamente los medios de procesamiento de la información.		

Cliente : Almacenes Si Van S.A. de C.V.
Auditoría : Auditoría Interna a las Tecnologías de Información
Periodo : Del 01 de Enero al 31 de Diciembre 2016

Programa de Auditoría Interna con Base a Buenas Prácticas

Preparado por: **Fecha:**
Revisado por : **Fecha:**
Aprobado por : **Fecha:**

C. Área:	Ventas		
N°	**Naturaleza o alcance de los procedimientos de auditoría**	**Ref. Pts.**	**Elaborado por**
1	Desarrolle una inspección accediendo a la página web del proveedor del sistema que se utiliza y verifique si la empresa posee la última versión de este, evidenciando mediante una captura de pantalla con dicha información, de no encontrarse la información en la página web, solicitarla al proveedor por medio de una confirmación externa		
2	Inspeccione si dentro de los reportes que emite el sistema genera reportes de las ventas realizadas en el día, realizando un listado de la información que muestra dicho reporte.		
3	Elabore una narrativa que detalle si el sistema genera las fechas y hora de las transacciones que se realizan.		
4	Inspeccione los reportes y registros emitidos por el sistema y solicite al encargado del área el listado de los reportes que genera el mismo, confrontando los reportes obtenidos con el listado proporcionado.		
5	Determine si el sistema emite reportes de las ventas realizadas con comprobantes de crédito fiscal o facturas y deje evidencia mediante imágenes que hagan constar los reportes emitidos.		
6	Realice una observación para determinar si el sistema permite realizar una transacción sin haber llenado todo los campos obligatorios.		
7	Efectué una observación para comprobar la existencia de antivirus en las máquinas de la entidad, luego prepare un detalle en el que se muestre si los antivirus que se poseen son libres o pagados.		
8	Realice una observación para comprobar que el firewall del sistema operativo se encuentre activado.		
9	Inspeccione que las transacciones realizadas en el sistema son precisas, completas y válidas confrontando con la documentación impresa que se posee.		
10	Realice una observación para verificar si el sistema genera reportes sobre la forma de pago cuando se realiza una venta, luego prepare un detalle de los campos que presenta el reporte.		

N°	Naturaleza o alcance de los procedimientos de auditoría	Ref. Pts.	Elaborado por
11	Realice una indagación con el personal clave del departamento para establecer si se poseen políticas para el aseguramiento y resguardo de los equipos informáticos, luego de establecer si cuentan con políticas solicite los documentos de las mismas.		
12	Efectué una indagación con el personal para evidenciar si la empresa tiene sus propios dispositivos de almacenamiento y si estos se encuentran encriptados.		
13	Indague con el encargado del área si la entidad cuenta con póliza de seguro para el equipo de la empresa, luego inspeccione los documentos y elabore una lista de los equipos que se encuentran cubiertos por dichas pólizas.		
14	Realice una observación al sistema para verificar si al memento de realizar una transacción electrónica cuenta con campos obligatorios para realizar la transacción, evidenciando mediante una captura de pantalla al realizar la prueba.		
15	Verifique si se cuentan con documentos de requerimientos de confidencialidad o acuerdos de no divulgación y solicite los mismos al responsable de dichos documentos.		
16	Indague con el personal para comprobar si se poseen políticas en las que se establezcan medidas de seguridad en el uso del sistema, confidencialidad y control interno, obtenga la documentación donde se encuentren establecidas.		
17	Indague con el personal del área si el sistema posee la protección adecuada en el comercio electrónico que se transmite a través de redes públicas ante cualquier actividad fraudulenta y elabore una narrativa detallando los tipos de protección que se poseen.		
18	Efectué una inspección en las instrucciones de manejo de errores que posee el sistema para verificar si las mismas son comprensibles para el personal, luego prepare una lista detallando las deficiencias encontradas si las hubiere.		
19	Indague con el encargado del área para identificar si la empresa posee políticas sobre usos inadecuados de los activos, luego inspeccione las políticas y realice un detalle de las deficiencias que se identifiquen.		
20	Indague si se cumplen los estándares de seguridad aplicables para la recepción, procesamiento, almacenamiento y salida de datos y enliste cada uno de los estándares que se aplican.		
21	Efectué una observación para corroborar si el departamento cuenta con controles de seguridad que restringen el acceso de personal no autorizado al sistema, luego mediante una narrativa detalle los controles que se poseen.		

N°	Naturaleza o alcance de los procedimientos de auditoría	Ref. Pts.	Elaborado por
22	Efectué una inspección a la información almacenada en formato electrónico para verificar si los procedimientos de resguardo de la información son los adecuados.		
23	Efectué una indagación con el personal de área para comprobar si se poseen planes de contingencia ante cualquier incidente que perjudique las operaciones del sistema y realice un listado detallando las contingencias con que poseen.		
24	Realice una indagación para identificar si se efectúan evaluaciones periódicas para monitorear y revisar las condiciones de seguridad de los sistemas y elabore una narrativa donde detalle la forma en que se realizan las evaluaciones y la periodicidad de las mismas.		
25	Efectué una indagación para determinar si el departamento cuenta con controles de detección de amenaza y la efectividad de los mismos, además solicite la documentación de dichos controles.		
26	Efectué una observación comprobando si existen restricciones en la instalación de programas en los equipos utilizados por el personal, desarrolle una narrativa describiendo las restricciones que existen y quienes se encuentran autorizados para instalar programas en los dispositivos.		
27	Verifique si se posee un navegador determinado para acceder al sistema en línea y detalle las restricciones que el navegador tiene.		
28	Efectué una indagación con el personal para determinar si el sistema cuenta con software para la detección de códigos maliciosos, evidenciando mediante capturas de pantalla los software instalados en los equipos.		
29	Inspeccione la página web de la entidad para verificar si está posee un encriptado para proteger la información que se transfiere desde el sitio, luego prepare un detalle del tipo de encriptado que se utiliza en la página.		
30	Desarrolle una indagación para establecer si el departamento cuenta con los debidos controles de seguridad física para el resguardo de los activos y elabore una lista de chequeo de los activos resguardados.		
31	Elabore cédula de detalle que muestre un extracto de las pólizas de seguros que la entidad posee para proteger las instalaciones, edificaciones y demás equipo.		
32	Indague si todos los bienes de la entidad están incluidos dentro de las pólizas adquiridas.		
33	Inspeccione en la página web de la entidad verificando si posee las certificaciones necesarias para el funcionamiento del sitio, solicite la documentación de las certificaciones al encargado del departamento.		

N°	Naturaleza o alcance de los procedimientos de auditoría	Ref. Pts.	Elaborado por
34	Compruebe si la empresa cuenta con la seguridad que permita conocer si algún individuo o grupo está ingresando en su red sin previa autorización, evidencie mediante capturas de pantallas las pruebas de seguridad realizadas.		
35	Determine cuál es el software que utiliza el departamento para proteger las contraseñas inalámbricas y limitar el acceso a la red wifi.		
36	Indague con el encargado del área si existen niveles jerárquicos en el acceso al sistema y elabore un listado detallando los distintos niveles de acceso con que cuentan.		
37	Corrobore si se implementa una distribución de los lineamientos y políticas de seguridad del departamento para todo el personal relacionado con el uso y manejo del sistema y elabore una cédula de detalle con todos los lineamientos y políticas que son proporcionados al personal.		
38	Inspeccione el sistema corroborando si este no permite realizar modificaciones, adiciones o eliminaciones a la información sin poseer la autorización necesaria, evidencie mediante capturas de pantallas las restricciones que presenta el sistema.		
39	Indague con el personal para determinar si este cuenta con formación regular para asegurar sus responsabilidades en el uso del sistema.		
40	Indague con el encargado del área si existen políticas para que los usuarios del sistema tengan los apropiados conocimientos de los controles de detección y prevención contra códigos maliciosos.		

Cliente : Almacenes Si Van S.A. de C.V.
Auditoría : Auditoría Interna a las Tecnologías de Información
Periodo : Del 01 de Enero al 31 de Diciembre 2016

Programa de Auditoría Interna con Base a Buenas Prácticas

Preparado por: **Fecha :**
Revisado por : **Fecha :**
Aprobado por : **Fecha :**

C. Área:	**Sistemas**		
N°	**Naturaleza o alcance de los procedimientos de auditoría**	**Ref. Pts.**	**Elaborado por**
1	Corrobore si el sistema que se utiliza es elaborado internamente y mediante narrativa documente los criterios para determinar la elaboración del sistema.		
2	Verifique si el sistema desarrollado está de acuerdo a los objetivos y necesidades de cada uno de los departamentos de la entidad.		
3	Indague si se poseen controles de acceso al código fuente de los programas.		
4	Indague en los contratos de adquisición de software y elabore una narrativa que detalle si se cumplen los derechos y obligaciones de todas las partes en los términos contractuales.		
5	Elabore narrativa que detalle si el departamento establece revisiones regulares del software y contenido de data del sistema, anexe la programación de revisiones y documente que se realicen de acuerdo a los periodos establecidos.		
6	Efectué una muestra de los equipo y verifique si se instalan y actualizan regularmente el software para la detección o reparación de códigos maliciosos		
7	Inspeccione si el sistema cuenta con limitaciones al número de intentos de registro infructuosos permitidos, detalle en una narrativa el proceso de ingreso al sistema y anexe bitácora de intentos de ingresos infructuosos.		
8	Elabore narrativa que exprese si el sistema cuenta con un control de acceso restringido a información confidencial.		
9	Verifique si se cuenta con procedimientos diseñados para proteger el intercambio de información de la intercepción, copiado, modificación, routing equivocado y destrucción de la misma, detalle en una narrativa los procedimientos que aplica.		

N°	Naturaleza o alcance de los procedimientos de auditoría	Ref. Pts.	Elaborado por
10	Verifique si la empresa cuenta con los siguientes controles de seguridad física para el resguardo de los activos: 1) Conexión eléctrica en buen estado 2) Los equipos están en un lugar fresco y en un mueble adecuado 3) El equipo debe estar limpio 4) Que no se desconecte ningún dispositivo si no se ha apagado el equipo.		
11	Inspeccione que todos los activos están claramente identificados y elabore un inventario físico del equipo que se posee.		
12	Compruebe si se implementan procedimientos para asegurar la integridad y consistencia de toda la información almacenada en formato electrónico, tales como bases de datos, almacén de datos y archivos de datos y mediante una narrativa detalle los procedimientos utilizados.		
13	Elabore narrativa que muestre si cuenta con políticas apropiadas para mantener legibles, fácilmente identificables y recuperables los registros que se encuentran en respaldos		
14	Verifique si se tienen lineamientos para detectar prontamente los errores en los resultados de procesamiento, detallando en una narrativa las actividades que se realizan para el procesamiento de datos.		
15	Elabore narrativa si posee controles de redundancia al momento de ingresar información al sistema.		
16	Indague por medio del encargado del departamento si cuenta con políticas para orientar a los empleados del tratamiento de los datos para evitar situaciones embarazosas para la empresa detalle por medio de narrativas las políticas implementadas.		
17	Inspeccione si se incorporan chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados, documente el proceso de validación de datos.		
18	Indague con el encargado del departamento si se cuenta con procedimientos para asegurar el rastreo y no repudio, mediante narrativa detalle los procedimientos utilizados.		
19	Detalle mediante narrativa si se cuenta con un conjunto de políticas de seguridad dirigidas a la gestión de redes y seguridad de los datos como parte de concientizar sobre los riesgos de las mismas		
20	Verifique si el sistema cuenta con jerarquía de contraseñas para el acceso al sistema, cuentas de administrador o invitados.		
21	Inspeccione si cuenta con directrices para la seguridad de la información y el sistema, dirigidas a usuarios ajenos a la entidad que tienen acceso al mismo en una narrativa exprese las directrices aplicables.		

N°	Naturaleza o alcance de los procedimientos de auditoría	Ref. Pts.	Elaborado por
22	Indague con el encargado del departamento si se cuenta con políticas para evitar el uso de información para lucro personal o que de alguna manera fuera contraria a la ley o en detrimento de los objetivos legítimos y éticos de la organización, detalle las políticas utilizadas por el departamento.		
23	Verifique si se cuentan con lineamientos específicos para la actualización de contraseñas como: 1) número de caracteres, 2)contraseñas que no sean únicas para todos los usuarios 3) que se guarden las contraseñas en los equipos		
24	Compruebe si se cuenta con un documento de políticas que este publicado y comunicado a todos los empleados y entidades externas relevantes y verifique que se encuentre aprobado por la gerencia, detalle en una narrativa las políticas y anexe el acuerdo de aprobación de la gerencia.		
25	Verifique si se guardan bitácora sobre fallas en el sistema para realizar las correcciones debidas posteriormente y mediante narrativa detalle las fallas.		
26	Elabore narrativa que detalle si se da seguimiento, analizan y se toma la acción apropiada en el caso de fallas al sistema.		
27	Inspeccione si se cuenta con planes de contingencia para solventar Intrusiones no deseadas al sistema.		
28	Verifique si se implementan planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos y detalle los planes que emplearía en caso de ocurrencia.		
29	Inspeccione si se cuentan con lineamientos que eviten el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la información documente los lineamientos en una narrativa.		
30	Inspeccione si se separan los medios de desarrollo, prueba y operacionales para reducir los riesgos de accesos no-autorizados o cambios en el sistema de operación y elabore un inventario de los equipos destinados para el desarrollo, prueba y uso operacional.		
31	Verifique si implementan medidas para la detección, prevención y actualización respecto a los parches de seguridad y control de firmas de virus para proteger los sistemas de información de un software malicioso, detalle las medidas que utiliza mediante narrativa.		
32	Realice narrativa si prepara, mantiene y comprueba planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente con un impacto de negocio grave.		

N°	Naturaleza o alcance de los procedimientos de auditoría	Ref. Pts.	Elaborado por
33	Inspeccione si se desarrollan e implementan planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos mediante narrativa detalle los planes que implementara en caso de ocurrencia.		
34	Compruebe si se poseen políticas formales prohibiendo el uso de software no-autorizado mediante acuerdo de la gerencia detalle la documentación de aprobación en una narrativa.		
35	Verifique que se preparen planes apropiados para la continuidad del negocio para recuperarse de ataques de códigos maliciosos y detalle los planes que se desarrollaran en caso de ocurrir un ataque.		
36	Compruebe si se realizan back-ups o respaldo de la información comercial y software esencial y se deben probar regularmente detalle en una narrativa los periodos de realización de pruebas de respaldo.		
38	Efectué una inspección y detalle mediante una narrativa si utiliza técnicas de codificación para proteger la confidencialidad, integridad y autenticidad de la información que se transmite electrónicamente.		
39	Inspeccione los contratos para verificar si se han establecidos acuerdos para el intercambio de información y software entre la organización y entidades externas.		
40	Inspeccione si se realizan registros de los intentos exitosos y fallidos de autenticación del sistema, mediante narrativa detalle la bitácora de intentos.		
41	Observe si se utilizan perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.		
42	Detalle en una narrativa si se protege la empresa mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.		
43	Verifique si las políticas de ingreso están establecidas de acuerdo al tamaño y estructura de la entidad y mediante una narrativa detallar las políticas de ingreso.		
44	Realice narrativa si se cuenta con políticas para uso de activos de tecnologías de información.		
45	Revise si los equipo cuentan con un dispositivo de suministro de energía ininterrumpido (UPS) para apagar o el funcionamiento continuo del equipo de soporte a las operaciones comerciales críticas		
46	Inspeccione si se cuenta con un generador de emergencia si se requiere que el procesamiento continué en el caso de una falla de energía prolongada		

N°	Naturaleza o alcance de los procedimientos de auditoría	Ref. Pts.	Elaborado por
47	Verifique si el cableado de la red está protegido contra intercepciones no autorizadas o daños		
48	Inspeccione si se permite a los usuarios empleados, contratistas y terceras personas el retiro de los activos fuera la institución, detalle mediante narrativa la política utilizada.		
49	Inspeccione que las redes están adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito elabore una narrativa que muestre que las redes están debidamente protegidas.		
50	Realice narrativa que exprese si poseen controles 'routing' para las redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso de las aplicaciones comerciales.		
51	Realice una inspección y elabore una narrativa que documente que se realizan revisiones al trabajo de los contratistas.		
52	Inspeccione si se establecen, acuerdan y comunican roles y responsabilidad de acceso a la red, detalle en una narrativa los roles dentro de acceso a la red y anexe los documentos que aparan los acuerdos y responsabilidades de acceso a la red.		
53	Realice una inspección y detalle en una narrativa si el uso de las redes es adecuadamente manejada y controlada para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.		
54	Inspeccione si se cuentan con política para el uso de comunicación inalámbrica, tomando en cuenta los riesgos particulares involucrados detalle en una narrativa las políticas utilizadas.		
55	Elabore una narrativa que compare el recurso humano disponible y las actividades de mantenimiento a los equipos y al software para determinar si es acorde a las necedades empresariales.		
56	Inspeccione si se realizan evaluaciones al personal de mantenimiento del equipo de tecnologías de información para evaluar la actualización de sus conocimientos respecto al uso y cuidado de las tecnologías de información		
57	Compruebe mediante los expedientes de los empleados que todos los usuarios tengan un identificador singular (ID de usuario) para su uso personal y exclusivo.		
58	Verifique que se tengan políticas definidas claramente para realizar la terminación o cambio del empleo y mediante narrativa detalle el proceso de cierre de usuarios en caso de ocurrencia.		
59	Realice una inspección y elabore una narrativa en la que muestre las políticas de redundancia para ID de usuarios		

Cliente : Almacenes Si Van S.A. de C.V.
Auditoría : Auditoría Interna a las Tecnologías de Información
Periodo : Del 01 de Enero al 31 de Diciembre 2016

Programa de Auditoría Interna con Base a Buenas Prácticas

Preparado por : **Fecha :**
Revisado por : **Fecha :**
Aprobado por : **Fecha :**

C. Área:	**Mercadería**		
N°	**Naturaleza o alcance de los procedimientos de auditoría**	**Ref. Pts.**	**Elaborado por**
1	Indague si el sistema permite el acceso a diferentes áreas de la entidad y elabore un listado de las áreas a las que se posee acceso.		
2	Efectué una indagación para verificar si el sistema emite un correlativo de las órdenes de compras realizadas.		
3	Indague con el encargado del área para verificar si los reportes de inventarios emitidos por el sistema brindan la información necesaria para el uso de los usuarios y elabore un listado de los ítems que muestra el reporte.		
4	Observe el área donde se encuentra el equipo informático para verificar si se cuenta con equipo de prevención ante cualquier incidente, evidenciando mediante fotografías del equipo de prevención.		
5	Verifique si en el sistema se generan reportes mostrando las existencias de inventarios y la cantidad que se retira durante el día y elabore un listado con los campos que muestra el reporte.		
6	Compruebe si el equipo informático se encuentra ubicado en el lugar adecuado para un óptimo funcionamiento y desarrolle una narrativa detallando las condiciones donde se encuentra ubicado el equipo.		
7	Corrobore que el reporte de inventarios emitido por el sistema posee la misma información que el inventario físico, cotejando el reporte con las existencias en bodega		
8	Determine si los datos del inventario son ingresados al sistema de forma manual y evidencie mediante fotografías el ingreso de la información al sistema por el personal encargado.		
9	Indague con el personal si se poseen políticas de control de acceso al sistema, solicite dichas políticas al encargado del área.		
10	Determine mediante la técnica de observación si se controlan los cambios en los medios de procesamiento de información y elabore una narrativa detallando las formas en que controlan dichos cambios.		

N°	Naturaleza o alcance de los procedimientos de auditoría	Ref. Pts.	Elaborado por
11	Verifique si el sistema emite un reporte que muestre información de la hora, fecha y nombre del personal que accede al sistema.		
12	Observe si el sistema permite agregar o modificar datos de los clientes sin poseer la autorización necesaria.		
13	Inspeccione las políticas de acceso al sistema que posee el departamento y realice una observación para corroborar los accesos del personal a los módulos autorizados.		
14	Indague con el encargado del área si el sistema cierra cesión después de un periodo de inactividad y elabore una narrativa detallando el tiempo que permite estar inactivo antes de cerrar sesión y si el cierre se realiza de una forma segura.		
15	Inspeccione si los back-up que genera el sistema poseen toda la información necesaria para el departamento y realice un detalle de cada uno de los reportes que se respaldan.		
16	Corrobore con el encargado del área si se cuentan con usuarios personalizados para acceder al sistema, evidenciando mediante capturas de pantalla los distintos usuarios que poseen acceso.		
17	Verifique si los equipos de cómputo cuentan con los adecuados reguladores de voltaje, así como si estos están de acorde a la capacidad establecida para cada uno de ellos.		
18	Verifique si la información involucrada en el comercio se encuentra protegida con medidas de seguridad adecuadas y elabore una narrativa detallando las medidas de seguridad utilizadas para proteger la información.		
19	Indague si los equipos autorizados están debidamente conectados a la red.		
20	Verifique si existen contraseñas para que los usuarios accedan a una red y las restricciones que existen para evitar el ingreso a páginas no autorizadas.		
21	Compruebe si se realizan mantenimientos periódicos a los equipos y la regularidad con que son realizados.		
22	Inspeccione si se cuentan con políticas que establezcan capacitaciones a los empleados en el uso y cuidado del sistema informático y solicite las políticas al encargado del departamento.		

Cliente : Almacenes Si Van S.A. de C.V.
Auditoría : Auditoría Interna a las Tecnologías de Información
Periodo : Del 01 de Enero al 31 de Diciembre 2016

Programa de Auditoría Interna con Base a Buenas Prácticas

Preparado por : **Fecha** :
Revisado por : **Fecha** :
Aprobado por : **Fecha** :

A. Área:	Contabilidad		
N°	**Naturaleza o alcance de los procedimientos de auditoría**	**Ref. Pts.**	**Elaborado por**
1	Compruebe si el sistema utilizado en el departamento genera los estados financieros principales y realice un listado detallando los estados financieros emitidos.		
2	Verifique la capacidad de almacenamiento de datos del sistema y elabore una narrativa describiendo la capacidad, localización y si el sistema recupera información eliminada accidentalmente.		
3	Indague con el personal del área la precisión de los reportes emitidos por el sistema y si los mismos son comprensibles para su evaluación y uso de terceros.		
4	Elabore una narrativa detallando las pruebas que se realizan al momento de realizar actualizaciones a los sistemas.		
5	Inspeccione si se cuenta con la documentación de la adquisición de los sistemas contables, solicite la misma al personal encargado.		
6	Verifique si se poseen controles de la salida de los equipos fuera de las instalaciones de la empresa en caso de reparación o para uso de usuarios de la entidad y elabore una narrativa detallando los controles que se aplican.		
7	Observe si el sistema muestra redundancias al momento de ingresar la información, evidencie mediante capturas de pantalla al sistema.		
8	Inspeccione los contratos de adquisición de los diferentes sistemas utilizados en el departamento, para identificar cualquier incumplimiento por ambas partes.		
9	Inspeccione en el manual de políticas proporcionadas por el departamento de TI, si se establece que no se pueden instalar software dentro de los sistemas operacionales sin previa autorización, seleccione de manera aleatoria un equipo y probar que no se pueden instalar software sin previa autorización.		
10	Indague con el encargado si el sistema permite importar y exportar datos hacia otros programas.		

N°	Naturaleza o alcance de los procedimientos de auditoría	Ref. Pts.	Elaborado por
11	Verifique si el sistema solicita autorización para realizar modificaciones dentro del sistema en periodos anteriores, deje evidencia mediante una instantánea del sistema solicitando la contraseña correspondiente.		
12	Indague si existen fallas en los reportes emitidos por el sistema y si existen medidas para solucionar los errores que se presenten.		
13	Solicite al departamento los reportes de los backups realizados, y seleccione aleatoriamente un backup, para inspeccionar y realizar la prueba verificando que se han generado de manera adecuada y ante cualquier necesidad funcionan correctamente.		
14	Solicite al encargado del departamento, reporte de las últimas actualizaciones instaladas a los sistemas utilizados e inspeccione si esta coincide con la instalada en los equipos utilizados.		
15	Observe en los equipos para comprobar si se cuentan con las licencias de uso de los sistemas operativos.		
16	Indague si las actualizaciones que se realizan al sistema son efectivas y realizadas oportunamente.		
17	Efectué una indagación para verificar si el acceso a los sistemas se encuentra jerarquizado y elabore un listado detallando la jerarquización existente.		
18	Compruebe si el sistema es compatible con cualquier sistema operativo y efectué una prueba para corroborar la compatibilidad del mismo.		
19	Indague si el sistema se encuentra vinculado a otros departamentos y el acceso que estos poseen en el sistema, deje evidencia mediante una instantánea de los accesos que poseen los otros departamentos.		
20	Indague si los accesos que poseen los usuarios de otras áreas al sistema pueden dañar o modificar la información que presenta y elabore una narrativa detallando los accesos a los módulos que poseen.		
21	Inspeccione si se pueden realizar modificaciones a la información de sucesos pasados y realice un detalle de la forma en que se clasifica la información.		
22	Verifique si los equipos de cómputo cuentan con los adecuados reguladores de voltaje, así como si estos están de acorde a la capacidad establecida para cada uno de ellos.		
23	Verifique mediante la técnica de observación si el acceso al equipo de cómputo cuenta con medidas de seguridad adecuadas.		
24	Corroboré el acceso de los usuarios a las redes compartidas, mediante la inspección de las computadoras conectadas vía LAN y vía WLAN.		

N°	Naturaleza o alcance de los procedimientos de auditoría	Ref. Pts.	Elaborado por
25	Solicite un detalle de los usuarios del sistema y los accesos que poseen a los distintos módulos del mismo, e inspeccione si los accesos están acorde a las funciones detalladas en el manual de funciones de puestos.		
26	Solicite los reportes de conciliación de saldos utilizados y verifique si existen situaciones que se deban de investigar para prevenir, detectar y dar repuesta a cualquier riesgo.		
27	Realice una solicitud del manual de políticas al departamento e indague si las mismas han sido divulgadas de manera adecuada al personal involucrado.		

Cliente : Almacenes Si Van S.A. de C.V.
Auditoría : Auditoría Interna a las Tecnologías de Información
Periodo : Del 01 de Enero al 31 de Diciembre 2016

Programa de Auditoría Interna con Base a Buenas Prácticas

Preparado por : **Fecha :**
Revisado por : **Fecha :**
Aprobado por : **Fecha :**

C. Área:	**Compras**		
N°	**Naturaleza o alcance de los procedimientos de auditoría**	**Ref. Pts.**	**Elaborado por**
1	Elabore narrativa sobre la adquisición software explique si la entidad posee procedimientos que hagan cumplir los derechos y obligaciones pactadas en el contrato.		
2	Elabore una narrativa exponiendo si los procedimientos de adquisición de activos están conforme a las políticas establecidas por la entidad.		
3	Inspeccione con qué frecuencia se efectúan revisiones de mantenimiento al equipo utilizado por el equipo de compras y elabore una narrativa el tiempo transcurrido entre una revisión y otra y el proceso utilizado para la realización del mantenimiento.		
4	Inspeccione el procedimiento para la adjudicación de servicios de mantenimiento para equipos de la entidad, elabore una narrativa mencionando si los procesos utilizados son los más adecuados y los de menor coste para empresa.		
5	Verifique que todos los equipos del departamento de compras con el objeto de asegurar su continua disponibilidad e integridad y para evitar fallos futuros.		
6	Verifique si se poseen documentos de respaldo de cada adquisición de activo fijo que se ha dado en la entidad, elabore una narrativa en la cual se detalle si existe información de respaldo en caso de ser necesaria para exigir una garantía sobre los equipos.		
7	Inspeccione si al adquirir un nuevo equipo informático haya sido proporcionado por el proveedor un manual donde especifique los controles de seguridad que la entidad debe seguir, detallar en una narrativa si se cumplen los procedimientos establecidos en los manuales.		
8	Indague con el encargado del departamento de compras si en las adquisiciones de equipos o de software el proveedor proporciona un periodo de prueba en el cual se puedan detectar fallas o insuficiencias que puedan ser riesgosas para la entidad en el futuro.		

N°	Naturaleza o alcance de los procedimientos de auditoría	Ref. Pts.	Elaborado por
9	Solicite una lista de activos fijos utilizados en el departamento de compras y cotéjelo con los códigos que posee cada equipo con el objeto de verificar que todos los dispositivos y muebles que han sido proporcionados no hayan sido extraviados.		
10	Elabore narrativa exponiendo si la empresa cuenta con políticas de resguardo y aseguramiento de los datos almacenados de las compras.		
11	Verifique si los encargados del departamento de compras comprueban con regularidad las copias de respaldo guardadas, elabore narrativa del proceso de comprobación.		
12	Inspeccione si la entidad utiliza firmas electrónicas para la autenticidad de pagos en línea que realice, elabore narrativa sobre el proceso realizado.		
13	Indague sobre la existencia de políticas para el uso de controles criptográficos que protejan la información.		
14	Realice una prueba en los dispositivos de la entidad, verificando si solicitan el ingreso de contraseñas para proporcionar acceso a información guardada en esto.		
15	Solicite a un empleado del departamento de compras que acceda con su usuario y contraseña al sistema y verifique que tenga acceso a los servicios para los cuales hayan sido autorizados previamente.		
16	Inspeccione si los contratos con proveedores tratan sobre requerimientos de seguridad y elabore una narrativa si dichos requisitos están conforme a los identificados por la entidad.		
17	Observe las restricciones para la instalación de programas en los equipos del departamento de compras, elabore una narrativa con las alertas presentadas al momento de instalar un programa ajeno a los utilizados en la entidad.		
18	Verifique que los controles de seguridad sobre equipos adquiridos, sean conforme a políticas establecidas por la entidad.		
19	Indagar con las personas encargadas del departamento de compras que los equipos adquiridos recientemente hayan sido entregados por el proveedor de manera adecuada y conforme al contrato pactado con la entidad.		
20	Inspeccione si en el departamento de compras poseen extintores para casos de emergencia y elabore una narrativa en la que se explique las fechas de recarga de cada extintor ubicado en el departamento.		
21	Verifique si en el departamento de compras se observan señalizaciones de rutas de escape en casos de emergencia así como también de señalización para puntos de encuentro.		
22	Indague los mecanismos utilizados por la entidad para la transmisión y recepción segura de datos y elabore una narrativa explicando los procedimientos utilizados.		

N°	Naturaleza o alcance de los procedimientos de auditoría	Ref. Pts.	Elaborado por
23	Inspeccione que solo dispositivos propios de la entidad pueden tener acceso a la red empresarial, desarrolle una narrativa en la cual exprese el proceso para poder acceder a la red empresarial.		
24	Verifique si el sistema del departamento está vinculado a otros sistemas de la entidad, comprobando el tipo de seguridad que este proceso tiene respecto a la información que se transfiere.		
25	Elabore una narrativa en la cual se exprese si se aplican los protocolos de seguridad aprobados por la entidad para las conexiones de red utilizadas.		
26	Verifique si los empleados aceptan y firman en su contrato las responsabilidades y la de la organización respecto a la seguridad de la información de la empresa.		
27	Indague si los encargados del departamento de compras poseen capacitaciones respecto al software que ellos utilizan, elabore una narrativa detallando los puntos de capacitaciones que los empleados reciben.		

CONCLUSIONES

- Se determinó posteriormente de la investigación que para llevar a cabo las actividades de auditoría interna poseen auditores con poca experiencia en el área, dado esto las auditorías a realizar se necesita contar con un criterio ya formado por los años de experiencia que tenga el auditor.
- La participación de la gerencia dentro de los procesos importantes en la entidad determina el grado de interés sobre ellos, esto contribuye a que el personal desarrolle de mejor manera las actividades asignadas, sin embargo en la investigación realizada la alta gerencia se involucra poco o nada en eventos relacionados con el sistema de gestión de la seguridad informática, dando lugar al poco interés por parte de los auditores internos facilitando el no evaluar al departamento de tecnologías de información que es un departamento de suma importancia para este tipo de empresas por la cantidad de información que se maneja dentro de los sistemas.
- Las actualizaciones sobre áreas pertinentes a las tecnologías de información y comunicación son importantes en el desarrollo de competencias del personal que ejecuta las auditorías internas, con el propósito que estas tengan los conocimientos mínimos necesarios sobre las áreas de seguridad física, seguridad lógica, redes y comunicaciones.
- Para desempeñar las actividades asignadas a las unidades de auditoría interna, los miembros de las mismas deben contar con los conocimientos necesarios sobre esta área, parte de ellos son los conocimientos en buenas prácticas, dichos conocimientos deben estar actualizados de manera constante a través de capacitaciones, sin embargo en las entidades comercializadoras de electrodomésticos la mayor parte de los

auditores interno han recibido su última capacitación sobre el tema hace más de tres años, generando así la realización de auditorías de manera desactualizada lo que conlleva a no realizar auditorías en áreas actuales o realizarlas con lineamientos antiguos que no ayudan a generar valor a los procesos.

- La debilidad que existe en la aplicación de las buenas prácticas y el poco conocimiento de los profesionales en el área de tecnologías de información y comunicación, genera vulnerabilidades dentro de las empresas debido a la escasa realización de auditorías al departamento de informática, no poseer la documentación correcta de las auditorías realizadas y no tomar en cuenta los procesos importantes y tareas en los programas de auditorías realizados.
- Sin un plan de contingencias hacia el uso, cuidado, mantenimiento y resguardo del activo tecnológico el área de informática se encuentra expuesta ante las amenazas cibernéticas que surgen constantemente.
- La falta de jerarquización en los accesos a los sistemas pone en riesgo la información de los clientes con que cuenta la empresa, dejándola de esta forma vulnerable a cambios indebidos en los sistemas.

RECOMENDACIONES.

- Se recomienda a las unidades de auditoría interna incluir dentro del perfil adecuado para esta área, poseer una experiencia de tres años en el área de auditoría interna, para que esto contribuya a un mejor desarrollo de las actividades pertinentes de dicha unidad, ya que el auditor ya cuenta con dicha práctica en el área.
- La alta gerencia de las entidades debe involucrarse en los eventos sobre el sistema de gestión de la seguridad informática de manera periódica, para contribuir al desempeño de las actividades de las unidades de auditoría interna.
- Los auditores internos para llevar a cabo auditorías al departamento de informática debe contar con los conocimientos sobre las áreas de seguridad física, seguridad lógica, redes y comunicaciones, por ello se le recomienda realizar capacitaciones sobre las mismas, así como también actualizar dichos contenidos en caso de ocurrir cambios, esto con el fin de realizar auditorías internas en esta áreas agregando valor a los procesos evitando así posibles daños.
- Para que las unidades de auditoría interna lleven a cabo sus actividades, se recomienda llevar a cabo actualizaciones sobre los conocimientos en buenas prácticas de manera constante de 2 veces al año como mínimo para profundizar más sobre los cambios que puedan generarse en el transcurso del tiempo.
- Todos los aspectos mencionados en el párrafo antecesor evidencian la necesidad que poseen los auditores de contar con procedimientos que les ayuden a evaluar al área de informática, con la aplicación de las buenas practicas, facilitando esto en gran manera una evaluación optima a dicho departamento, previniendo así las amenazas y

vulnerabilidades con las que se enfrenta dicho departamento con la evolución constante de la tecnología.

- Se recomienda que el personal de auditoría interna tome en cuenta los programas para realizar una evaluación al área de tecnologías de información y comunicación bajo el enfoque de buenas prácticas de tal forma que a través de estos se mitigué el riesgo en el activo tecnológico y en las áreas importantes de tecnologías de información y comunicación mediante la implementación de un sistema de seguridad.
- Crear accesos jerarquizados a la información que posee el área de tecnologías de información y comunicación, además establecer periodos para realizar una mejor evaluación al área.

BIBLIOGRAFÍA

Cortagerena, C. F. (2001). *Tecnologías de la información y las comunicaciones* . Sánchez de Loria 2251: Indugraf S.A. .

Instituto de Auditores Internos de España. (Marzo de 2015). Obtenido de http://www.kpmg.com/ES/es/servicios/Advisory/RiskCompliance/Cambio-Climatico-Sostenibilidad/Documents/vision-2020-20150323.pdf

Preparatorio Auditoría. (s.f.). *Auditoría de Cumplimiento*. Obtenido de CAPÍTULO6: https://preparatorioauditoría.wikispaces.com/Auditoría+de+Cumplimiento

Servicios TIC. (s.f.). *Definición de TIC*. Obtenido de Las T.I.C.: http://www.serviciostic.com/las-tic/definicion-de-tic.html

Significados. (s.f.). *Significado de Hardware*. Obtenido de Expresiones en inglés: http://www.significados.com/hardware/

ANEXOS

ANEXO 1: ENCUESTA

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

CUESTIONARIO

Dirigido: Los encargados de las unidades de auditoría interna de las empresas comercializadoras de electrodomésticos.

Propósito: La presente lista de preguntas ha sido elaborada por estudiantes de la carrera de licenciatura en contaduría pública, con el propósito de sustentar el trabajo de investigación "Programas de auditoría interna para realizar una evaluación al área de tecnologías de información bajo el enfoque de buenas prácticas en las empresas comercializadoras de electrodomésticos ubicadas en el área metropolitana de san salvador"

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

1. Sexo

1) Femenino ☐ 2) Masculino ☐

2. ¿Cuál es su profesión?

_____

Objetivo: Indagar acerca de la profesión a la cual pertenece el personal de auditoría interna.

Indicador: Perfiles profesionales.

3. ¿Cuánto tiempo tiene de ejercer la auditoría interna?

1) De 0 a 6 meses ☐

2) De 6 meses a 1 año ☐

3) De 1 a 3 años ☐

4) Más de 3 años ☐

Objetivo: Indagar el tiempo en que los auditores llevan desempeñando la profesión

Indicador: Perfiles profesionales

4. ¿Qué conocimientos tiene del área de informática y que le son aplicables en el contexto de su ejercicio?

1) COBIT 5 ☐

2) ISO ☐

3) ITAF ☐

4) Todas las anteriores y otras ☐

Objetivo: Conocer si ha realizado estudios académicos relacionados con el área de tecnologías de la información.

Indicador: Conocimientos normativos en materia de tecnologías de información.

5. ¿Conoce usted sobre la aplicación de las buenas prácticas al departamento de informática?

1) Sí ☐ 2) No ☐

Objetivo: Indagar sobre los conocimientos que posee el personal de auditoría interna para la aplicación de buenas prácticas al departamento de Informática.

Indicador: Conocimientos normativos en materia de tecnologías de información.

6. ¿Indique hace cuánto tiempo recibió su última capacitación en el área de buenas prácticas?

1) De 0 a 6 meses ☐

2) De 6 meses a 1 año ☐

3) De 1 a 3 años ☐

4) Más de 3 años ☐

Objetivo: Conocer el grado de actualización sobre el área de buenas prácticas.

Indicador: Capacitación del personal.

7. ¿Qué aéreas de tecnologías de información y comunicación ha recibido en las capacitaciones?

1) Seguridad Física ☐

2) Seguridad Lógica ☐

3) Redes y Comunicaciones ☐

4) Otras ☐

Objetivo: Conocer las diferentes aéreas en las que la gerencia capacita al personal de auditoría interna.

Indicador: Capacitación del personal.

8. ¿El acceso a los sistemas se encuentra jerarquizado?

1) SI ☐ 2) NO ☐

Objetivo: Determinar si poseen controles de seguridad respecto al acceso a sistemas que se utilicen en la entidad.

Indicador: Políticas de la entidad aplicables al uso de tecnologías de información.

9. ¿Con que frecuencia la alta dirección participa en eventos relacionados con el sistema de gestión de la seguridad informática?

1) Mensualmente ☐

2) Cada seis meses ☐

3) Una vez al año ☐

4) Nunca participa ☐

Objetivo: Verificar la importancia que posee el departamento de informática para la gerencia de las empresas.

Indicador: Compromiso del gobierno corporativo.

10. ¿Qué tan consciente se encuentra el personal de auditoría interna de los objetivos del departamento de informática?

Muy consiente ☐

Consiente ☐

No conoce los objetivos ☐

Objetivo: Determinar el conocimiento que poseen los empleados del departamento de auditoría interna sobre los objetivos del departamento de informática para determinar el grado de compromiso que poseen en el desarrollo de ellos.

Indicador: Políticas de la entidad aplicables al uso de tecnologías de información.

11. ¿Posee el software más adecuado para el manejo de la información de los clientes?

1) SI ☐ 2) NO ☐

Objetivo: Indagar sobre los programas y software que poseen las empresas y lo actualizados que están en ellos.

Indicador: Conocimientos normativos en materia de determinación de riesgos en las tecnologías de información.

12. ¿Con qué frecuencia se realizan revisiones para determinar y eliminar causas de posibles daños a la entidad?

1) Mensualmente ☐

2) Cada seis meses ☐

3) Una vez al año ☐

4) Nunca ☐

Objetivo: Identificar si las empresas realizan revisiones a los equipos informáticos y con qué frecuencia realizan estas revisiones.

Indicador: Políticas de la entidad aplicables al uso de tecnologías de información.

13. ¿Qué tan frecuente son tomados en cuenta los procesos importantes y tareas en los programas de auditorías realizados?

1) Siempre son tomadas en cuenta ☐

2) Frecuentemente son tomadas en cuenta ☐

3) Nunca son tomados en cuenta ☐

Objetivo: Definir si los procesos importantes dentro de la institución se toman en cuenta a la hora de realizar auditorías.

Indicador: Planes de seguimiento.

14. ¿Qué tan documentados están los registros del proceso de auditoría interna?

1) Muy bueno ☐

2) Bueno ☐

3) No están documentados ☐

Objetivo: Comprobar si los registros de auditoría interna se encuentran documentados correctamente.

Indicador: Planes de seguimiento.

15. ¿Se realizan auditorías internas al departamento de tecnologías de información?

1) Sí ☐ 2) No ☐

Objetivo: Comprobar si la unidad de auditoría interna realiza auditorías al departamento de tecnologías de información.

Indicador: Implementación de los programas.

16. ¿Qué tan frecuentemente se realizan auditorías internas al departamento?

1) Cada año ☐

2) Cada dos años ☐

3) Tres años o más. ☐

Objetivo: Conocer que tan frecuentemente se realizar auditorías internas al departamento de Informática.

Indicador: Planes de seguimiento.

17. ¿El departamento de auditoría interna posee periodos establecidos para la realización de auditorías internas a la unidad de tecnologías de información?

1) Cada mes ☐

2) Semestralmente ☐

3) Anual ☐

4) Nunca ☐

Objetivo: Conocer el periodo sobre el cual se realizan evaluaciones al departamento de tecnologías de investigación.

Indicador: Planes de seguimiento.

18. ¿Qué tan frecuente se realizan auditorías internas del sistema de gestión de la seguridad de la información (SGSI) en los periodos establecidos?

1) Cada mes ☐

2) Semestralmente ☐

3) Anual ☐

4) Nunca ☐

Objetivo: Verificar si el departamento de auditoría interna evalúa el sistema de gestión de la seguridad de la información.

Indicador: Conocimientos normativos en materia de determinación de riesgos en las tecnologías de información.

19. ¿Se cuentan con procedimientos que evalúen el uso, cuidado y mantenimiento de los activos tecnológicos de la empresa?

1) SI ☐ 2) NO ☐

Objetivo: Verificar si la unidad de auditoría interna cuenta con programas para la evaluación del uso, cuidado y mantenimiento de los activos tecnológicos de la entidad.

Indicador: Conocimientos normativos en materia de determinación de riesgos en las tecnologías de información.

20. ¿Estaría usted dispuesto a utilizar una propuesta de los programas de auditoría interna que contemplen la evaluación de T.I. bajo el enfoque de buenas prácticas?

1) SI ☐ 2) NO ☐

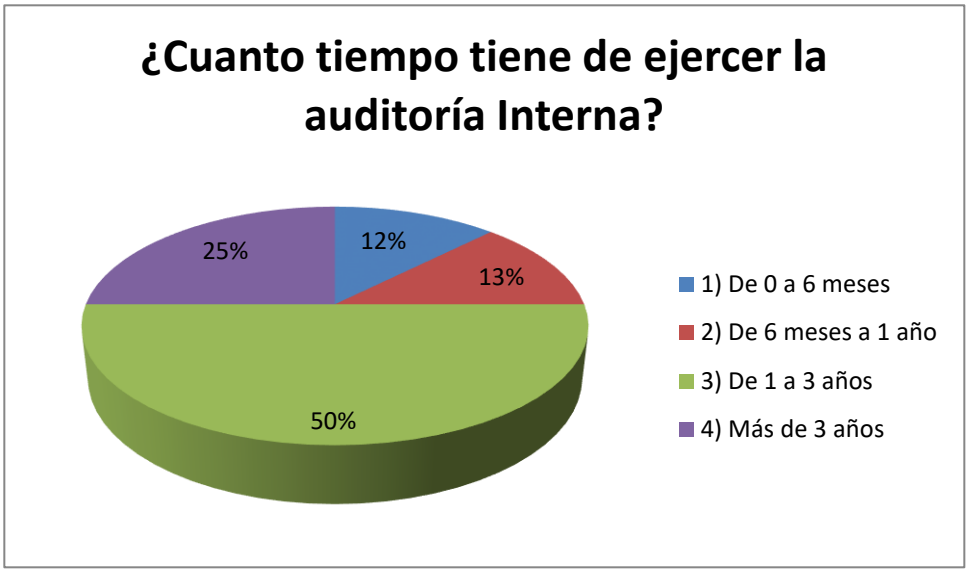
Objetivo: Determinar si el departamento de auditoría interna se encuentra interesado en poner en práctica los programas que se realizaran.

Indicador: Implementación de los programas.

ANEXO 2: Tabulación y análisis de datos

3. ¿Cuánto tiempo tiene de ejercer la auditoría interna?

Objetivo: Indagar el tiempo en que los auditores llevan desempeñando la profesión



Alternativa	Fr.	Fr. %
1) De 0 a 6 meses	2	13%
2) De 6 meses a 1 año	2	13%
3) De 1 a 3 años	8	50%
4) Más de 3 años	4	25%
	16	**100%**

Análisis:

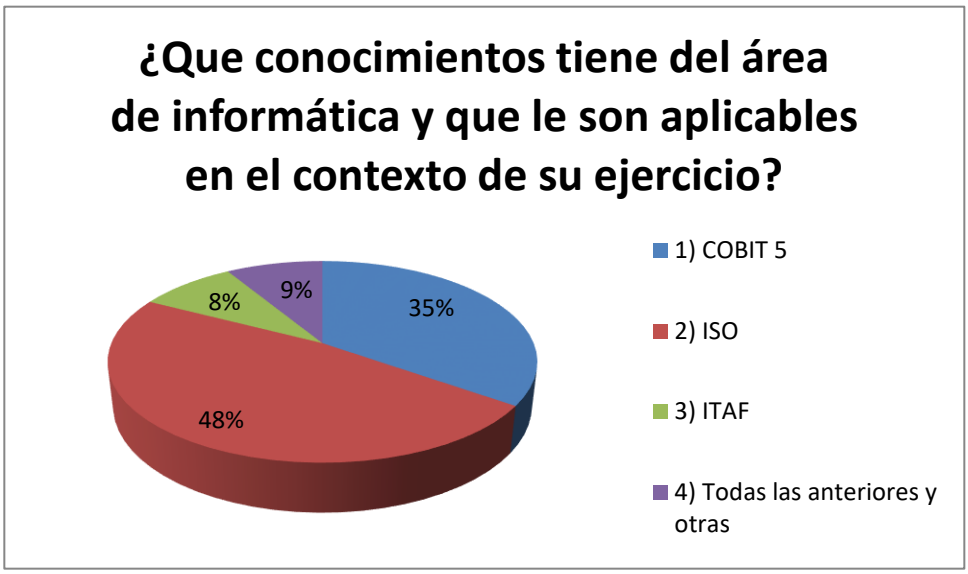
Dentro de los aspectos a evaluar para el perfil del recurso humano de las unidades de auditoría interna esta la experiencia que poseen los auditores internos, esto marca un parámetro para realizar las actividades asignadas.

El tiempo de experiencia de los auditores influye de manera importante en las actividades de las unidades de auditoría interna debido a que una de las causas de porque no se realizan auditorías al área de tecnología de información es la falta de experiencia en este caso según la información recopilada, solo el13% de los encuestados posee una experiencia de 0 a 6 meses en el aérea, sin embargo la mayoría de auditores internos posee una experiencia de 1 a 3 años dando como resultado que el 50% de los auditores entrevistados, los auditores con una mayor experiencia son de 25% de la población estudiada.

Esto nos da como resultado que el 75% de los auditores tienen una experiencia mayor a un año, teniendo así mayores conocimientos sobre auditoría interna, las buenas prácticas y por ente tecnologías de información, sin embargo en los datos resultantes de las preguntas 5 y 6 nos da como resultado que efectivamente la mayoría de los encuestado conoce sobre la aplicación de las buenas prácticas en un 56%, pero estos conocimientos no se encuentran actualizados debido a que el 44% de los auditores recibió su última capacitación sobre el tema hace más de 3 años, dejando así conocimientos ambiguos así como nuevas técnicas y aéreas a evaluar como lo es el área de tecnologías de información

4. ¿Qué conocimientos tiene del área de informática y que le son aplicables en el contexto de su ejercicio?

Objetivo: Conocer si ha realizado estudios académicos relacionados con el área de tecnologías de la información.



Alternativa	Fr.	Fr. %
1) COBIT 5	8	35%
2) ISO	11	48%
3) ITAF	2	9%
4) Todas las anteriores y otras	2	9%
	23	**100%**

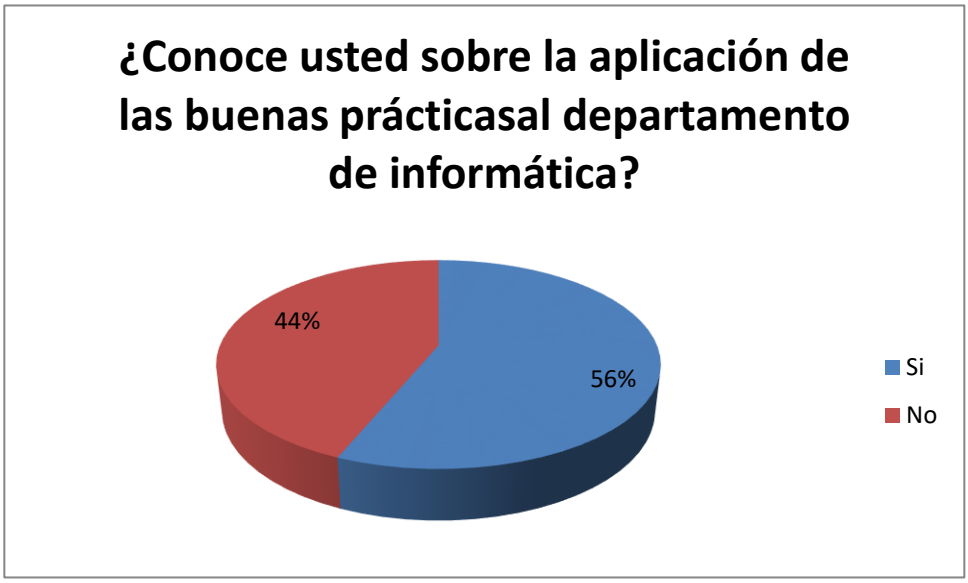
Análisis:

Para llevar a cabo una auditoría interna al área de tecnologías de información se necesita poseer conocimiento en normativa aplicable a dicha área, debido a que es un área especializada, dentro de los requerimientos para el perfil necesario dentro de la unidad de auditoría interna están los conocimientos en materia de tecnologías de información, ya que la falta de conocimiento de la normativa puede llegar a influir para la realización o no de las auditorías al departamento de tecnologías de información.

Entre la normativa aplicable que se necesita para realizar procedimientos de auditoría interna al área de tecnologías de información esta COBIT 5, ISO 27001 y 27002, e ITAF, no obstante según los resultados de los encuestados solo el 11% de ellos posee conocimiento de estas normativas aplicables, la mayoría posee conocimiento sobre la normativa ISO, dejando con menores conocimientos las normativas COBIT 5 e ITAF; la falta de conocimiento y dominio de las tecnologías de información son parte de las causas por las cuales los auditores internos no realizan auditorías a este departamento, sin embargo según los resultados obtenidos en la pregunta nº7 los auditores encuestados han recibido capacitaciones sobre aéreas de tecnologías de información, en su mayoría sobre seguridad de la información.

5. ¿Conoce usted sobre la aplicación de las buenas prácticas al departamento de informática?

Objetivo: Indagar sobre los conocimientos que posee el personal de auditoría interna para la aplicación de buenas prácticas al departamento de Informática.



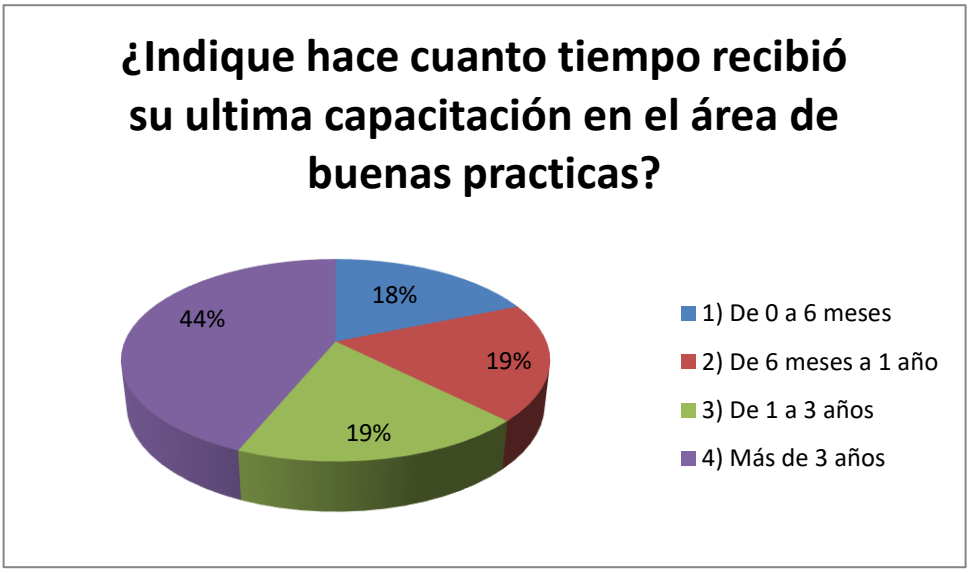
Alternativa	Fr.	Fr. %
Si	9	56%
No	7	44%
	16	**100%**

Análisis:
Dado que la auditoría interna es una actividad para generar valor y mejorar los procesos dentro de las empresas el conocimiento sobre la aplicación de buenas prácticas es de suma importancia para las unidades de auditoría interna.

Los resultados obtenidos de los encuestados en un 56% posee conocimientos sobre la aplicación de buenas prácticas al departamento de tecnologías de información versus un 44% que no posee conocimiento sobre ello, sin embargo en los obtenido en la pregunta Nº15 sobre la realización de auditorías al área de tecnologías de información el 81% de estas empresas no llevan a cabo auditorías de este tipo, lo que podemos concluir que dichos conocimientos no son aplicados, por la falta de conocimiento sobre la normativa técnica como se observa en los resultados de la pregunta Nº4.

6. ¿Indique hace cuánto tiempo recibió su última capacitación en el área de buenas prácticas?

Objetivo: Conocer el grado de actualización sobre el área de buenas prácticas.



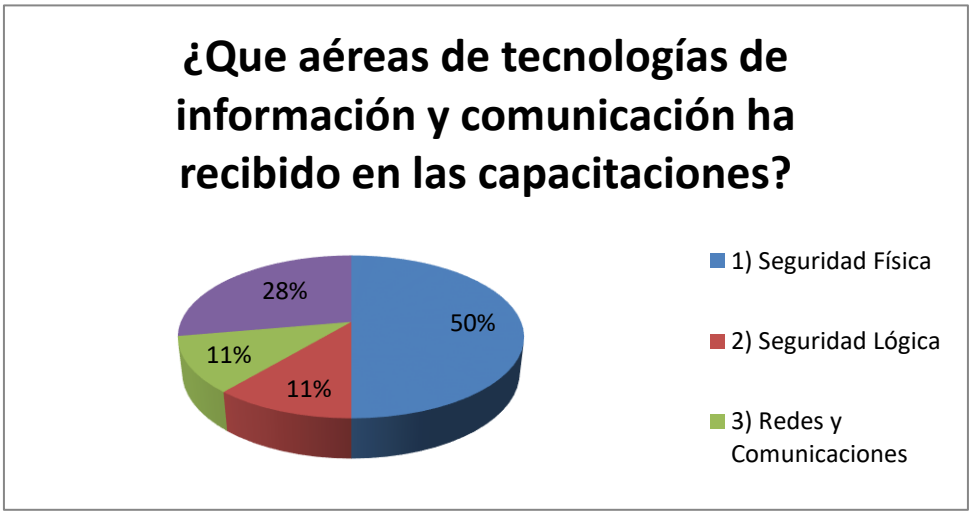
Alternativa	Fr.	Fr. %
1) De 0 a 6 meses	3	19%
2) De 6 meses a 1 año	3	19%
3) De 1 a 3 años	3	19%
4) Más de 3 años	7	44%
	16	**100%**

Análisis:

Para contribuir a los conocimientos y la aplicación de las buenas prácticas es necesario poseer actualizaciones constantes sobre el temas, no obstante la mayoría de auditores recibieron su última capacitación hace más de tres años en un porcentaje del 44%, lo cual es alarmante para llevar a cabo las actividades de auditoría interna de una manera deseada y eso no contribuye al mejoramiento de los procesos dentro de la entidad; los demás encuestados respondieron en un 19% para cada opción haber recibido estas capacitaciones de 0 a 6 meses, de 6 meses a 1 años y de 1 a 3 años.

7. ¿Qué áreas de tecnologías de información y comunicación ha recibido en las capacitaciones?

Objetivo: Conocer las diferentes aéreas en las que la gerencia capacita al personal de auditoría interna.



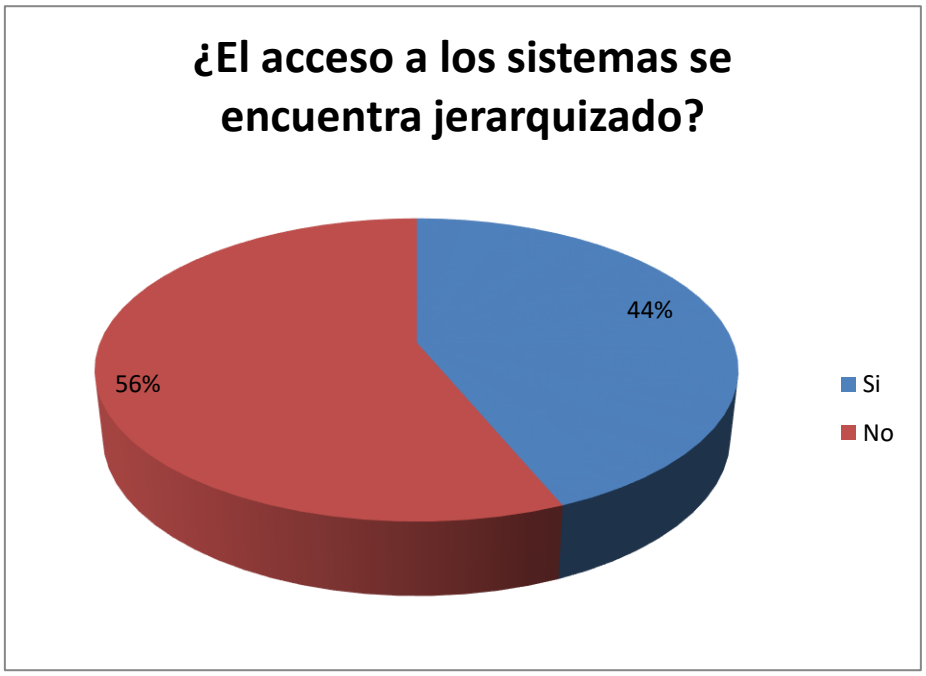
Alternativa	Fr.	Fr. %
1) Seguridad Física	9	50%
2) Seguridad Lógica	2	11%
3) Redes y Comunicaciones	2	11%
4) Otras	5	28%
	18	**100%**

Análisis:

Dentro de los conocimientos obtenidos por los auditores internos por medio de capacitaciones en su mayoría ha sido en seguridad física a las tecnologías de información que consta sobre el uso y cuidado que debe poseer al uso de tecnologías de información en un 50% de los entrevistados respondió haber recibido capacitaciones sobre esta área, dejando con un 11% capacitaciones sobre seguridad lógica y redes y comunicaciones, y en un 28% en otras capacitaciones sobre este tema, esto con el objetivo de medir que tan involucrada se encuentra la gerencia sobre la importancia de que los auditores estén en actualización constante de los conocimientos necesarios para llevar a cabo las actividades de auditoría en el área de tecnología de información.

8. ¿El acceso a los sistemas se encuentra jerarquizado?

Objetivo: Determinar si poseen controles de seguridad respecto al acceso a sistemas que se utilicen en la entidad.

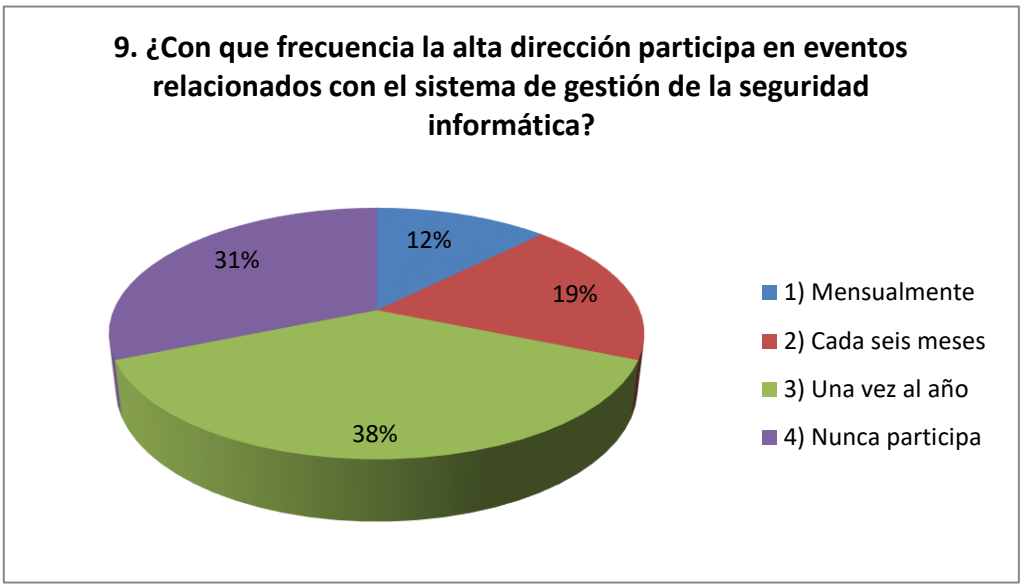


Alternativa	Fr.	Fr. %
Si	7	44%
No	9	56%
	16	**100%**

Análisis:
Debido que este tipo de empresas manejan por medio de sistemas computarizados sus operaciones es necesario que dichas compañías posean políticas de seguridad no solo física sino que también de manera lógica dentro de ellas, para proteger la información que carácter confidencial, así como registros, modificaciones entre otras como las intrusiones no deseadas al sistema las empresas deben contar con medidas de seguridad como la jerarquización de los sistemas la mayoría en un 56% de los encuestados respondieron no contar con jerarquización de los sistemas dejando libre acceso a los empleados sobre los datos del sistema.

9. ¿Con que frecuencia la alta dirección participa en eventos relacionados con el sistema de gestión de la seguridad informática?

Objetivo: Verificar la importancia que posee el departamento de informática para la gerencia de las empresas.



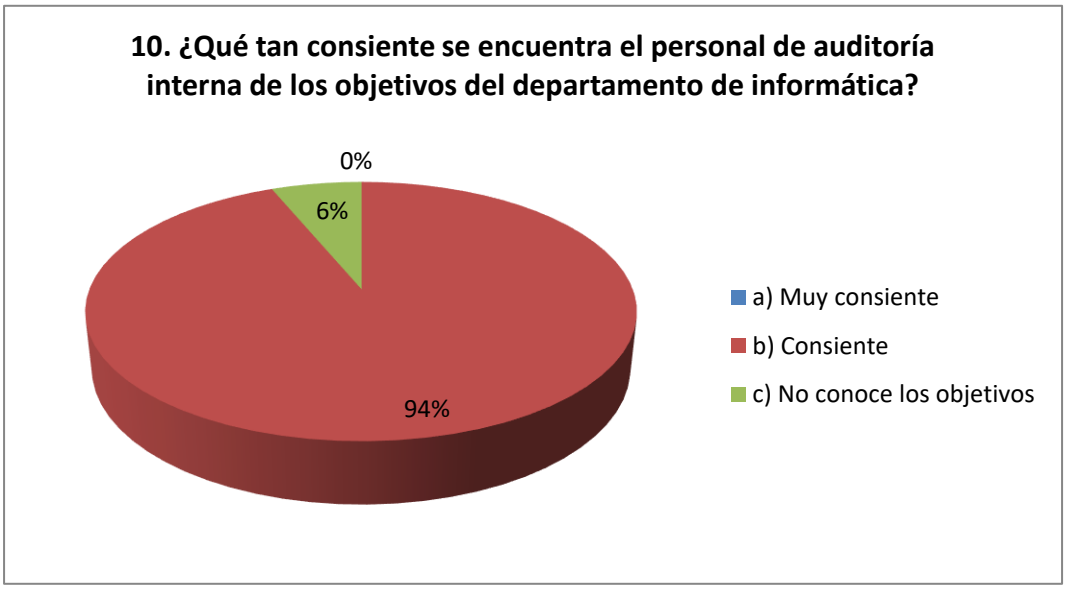
Alternativa	Fr.	Fr. %
1) Mensualmente	2	13%
2) Cada seis meses	3	19%
3) Una vez al año	6	38%
4) Nunca participa	5	31%
	16	100%

La seguridad informática es un factor del cual los gerentes deben de estar muy pendientes, ya que una falla en el sistema informático conlleva muchos riesgos entre los cuales se pueden mencionar, perdida de información confidencial, virus informáticos que afecten los ordenadores, error en procesos importantes, entre otros, por este motivo el gobierno corporativo debe poseer especial compromiso en el seguimiento al departamento de tecnologías de información.

Según la investigación realizada se determinó que solo un 13% de las empresas efectúan eventos los cuales están relacionados con la seguridad informática, es decir, para estas empresas es de suma importancia la realización y seguimiento de evaluaciones continuas al departamento de tecnologías de información, no siendo así para un 31% de las entidades encuestadas ya que estas nunca ejecutan procedimientos encaminados a la seguridad de la información, por otro lado, un 19% de las compañías toman en cuenta la seguridad informática ya que por lo menos cada 6 meses están en constante seguimiento en esta área, por ultimo podemos identificar que las organizaciones en las que sus gerentes participan en eventos relacionados a la seguridad de la información es un 38% del total de encuestados.

10. ¿Qué tan consiente se encuentra el personal de auditoría interna de los objetivos del departamento de informática?

Objetivo: Determinar el conocimiento que poseen los empleados del departamento de auditoría interna sobre los objetivos del departamento de informática para determinar el grado de compromiso que poseen en el desarrollo de ellos.



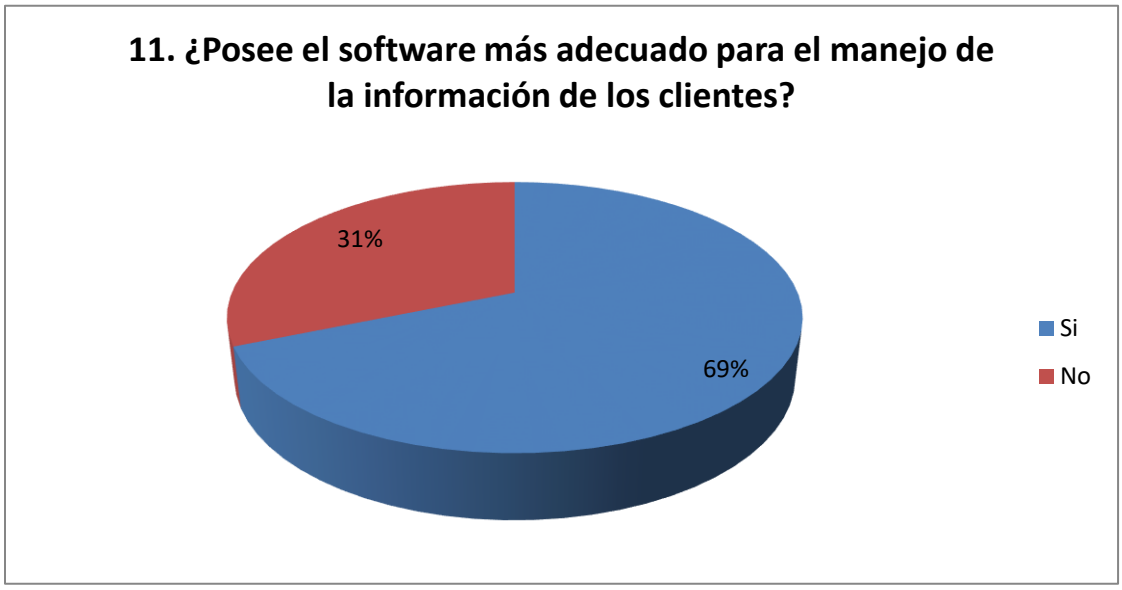
Alternativa	Fr.	Fr. %
a) Muy consiente	0	0%
b) Consiente	15	94%
c) No conoce los objetivos	1	6%
	16	100%

El departamento de auditoría interna por ser uno de sus roles la evaluación total de las empresas deben conocer los objetivos que persigue cada área de la entidad para poder realizar los procedimientos necesarios a la hora de ejecutar la auditoría como tal y plantear planes de seguimiento para cada departamento.

De los resultados que genero la realización de encuestas se puede observar que con un 94% la mayoría de las empresas poseen conciencia y conocimiento de los objetivos que persigue el departamento de tecnologías de información, en cambio un 6% que corresponde de las entidad encuestadas no conoce las objetivos del departamento.

11. ¿Posee el software más adecuado para el manejo de la información de los clientes?

Objetivo: Indagar sobre los programas y software que poseen las empresas y lo actualizados que están en ellos.



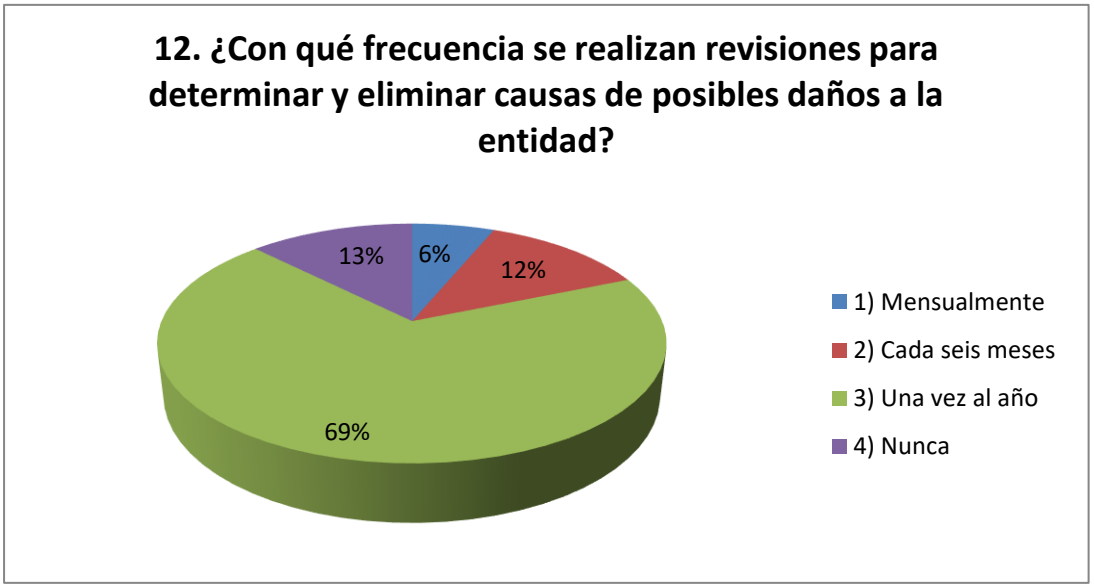
Alternativa	Fr.	Fr. %
Si	11	69%
No	5	31%
	16	100%

Uno de los factores que se evalúan al momento de la verificación de la seguridad de la información es el software que las empresas utilizan en sus labores cotidianas, poseer un software actualizado y seguro debe ser un política empresarial respecto al uso de las tecnologías de información para poder obtener los mejores resultados posibles y poseer la mayor confidencialidad de los datos de los clientes.

De las entidades encuestadas un 69% contesto que ellas poseen un software adecuado para el manejo de la información de los clientes lo que repercute en una buena administración de los datos confidenciales y de los procesos realizados, por otro lado se puede observar que un 31% no poseen el software más adecuado lo que debilita la seguridad y existe un mayor riesgo para la información.

12. ¿Con qué frecuencia se realizan revisiones para determinar y eliminar causas de posibles daños a la entidad?

Objetivo: Identificar si las empresas realizan revisiones a los equipos informáticos y con qué frecuencia realizan estas revisiones.



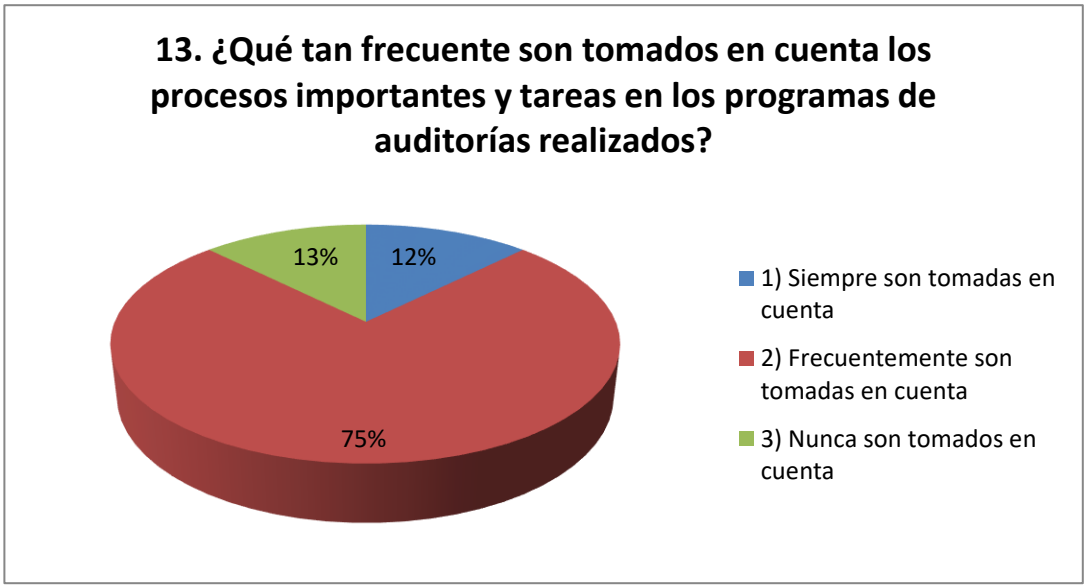
Alternativa	Fr.	Fr. %
1) Mensualmente	1	6%
2) Cada seis meses	2	13%
3) Una vez al año	11	69%
4) Nunca	2	13%
	16	100%

La auditoría interna debe tener constante seguimiento sobre los riesgos que puedan afectar a la entidad es por ello que se deben realizar constantemente evaluaciones que determines amenazas y que se puedan eliminar de forma adecuada.

Los resultados que dio la investigación determinó que un su mayoría y con un 69% las empresas realizan revisiones anualmente lo cual vulnera la seguridad de la información ya que no es posible identificar con suficiente tiempo amenazas que pueden afectar a la entidad, por otro lado se observa que un 13% de las empresas efectúan revisiones cada 6 meses y también un 13% de las entidades encuestadas nunca realizan revisiones para la determinación de posibles daños, de todos los encuestados solamente un 6% respondió que se ejecutan revisiones mensualmente, lo cual garantiza un mayor control de los riesgos y la determinación anticipada de las amenazas que afecten a la organización.

13. ¿Qué tan frecuente son tomados en cuenta los procesos importantes y tareas en los programas de auditorías realizados?

Objetivo: Definir si los procesos importantes dentro de la institución se toman en cuenta a la hora de realizar auditorías.



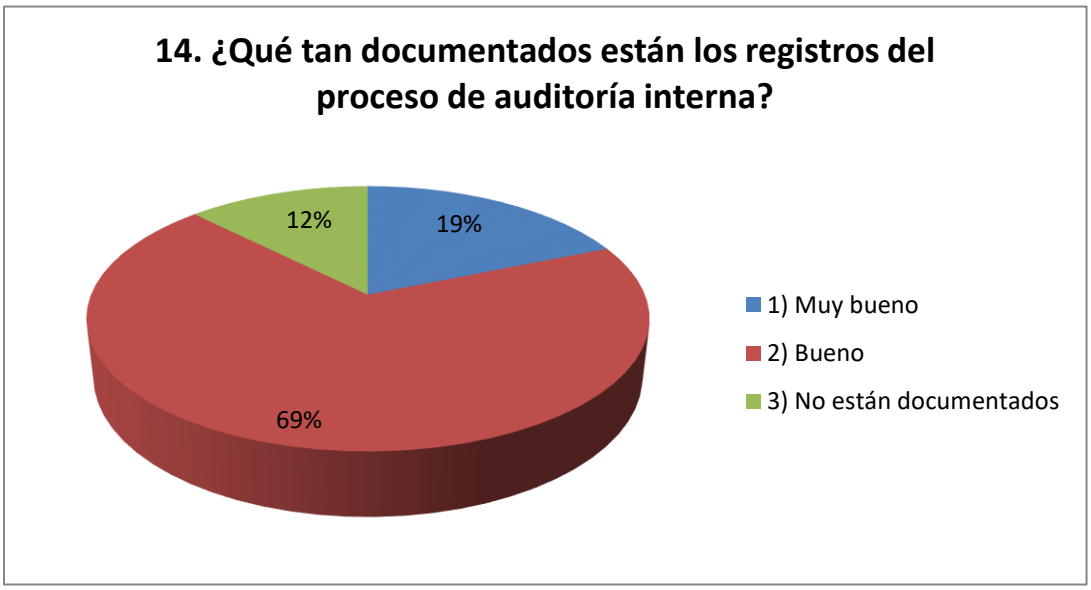
Alternativa	Fr.	Fr. %
1) Siempre son tomadas en cuenta	2	12.50%
2) Frecuentemente son tomadas en cuenta	12	75.00%
3) Nunca son tomados en cuenta	2	12.50%
	16	100%

Los procesos importantes dentro de cada departamento de la empresa deben ser tomados en cuenta para realizar los programas de auditoría ya que de esta manera se sabe a qué tomarle mayor importancia y a que procesos se le debe dar mayor seguimiento.

Según los resultados de la encuesta un 75% de las empresas investigadas toman en cuenta frecuentemente los procesos y las tareas importantes del departamento de tecnologías de información, mientras que con 12.5% los auditores internos en la elaboración de los programas utilizados toman en cuentan los procesos importantes, así mismo con un 12.5% de las empresas encuestadas, los auditores internos no toman en cuenta los procesos y tareas del departamento de informática.

14. ¿Qué tan documentados están los registros del proceso de auditoría interna?

Objetivo: Comprobar si los registros de auditoría interna se encuentran documentados correctamente.



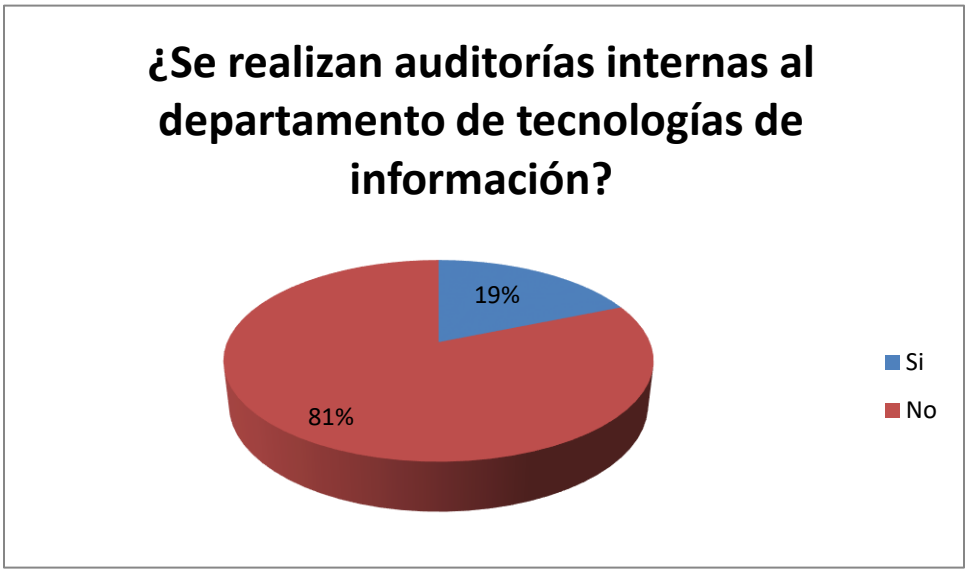
Alternativa	Fr.	Fr. %
1) Muy bueno	3	19%
2) Bueno	11	69%
3) No están documentados	2	13%
	16	100%

Para todos los programas de auditoría que se ejecuten en cada revisión estos deben ser evidenciados por documentos de respaldos e información que ayuden a sustentar todos los procedimientos que el auditor realizo.

Según los datos recabados en la ejecución de las encuestas observamos que un 19% poseen un muy buen respaldo de los procedimientos efectuados, por otra parte y con un 69% los auditores internos respondieron que sus procedimientos están documentados de una forma buena, y con un 13% de respuestas se observa que los procesos de auditoría no están documentados en ninguna forma.

15. ¿Se realizan auditorías internas al departamento de tecnologías de información?

Objetivo: Comprobar si la unidad de auditoría interna realiza auditorías al departamento de tecnologías de información.



Alternativa	Fr.	Fr. %
Si	3	19%
No	13	81%
	16	100%

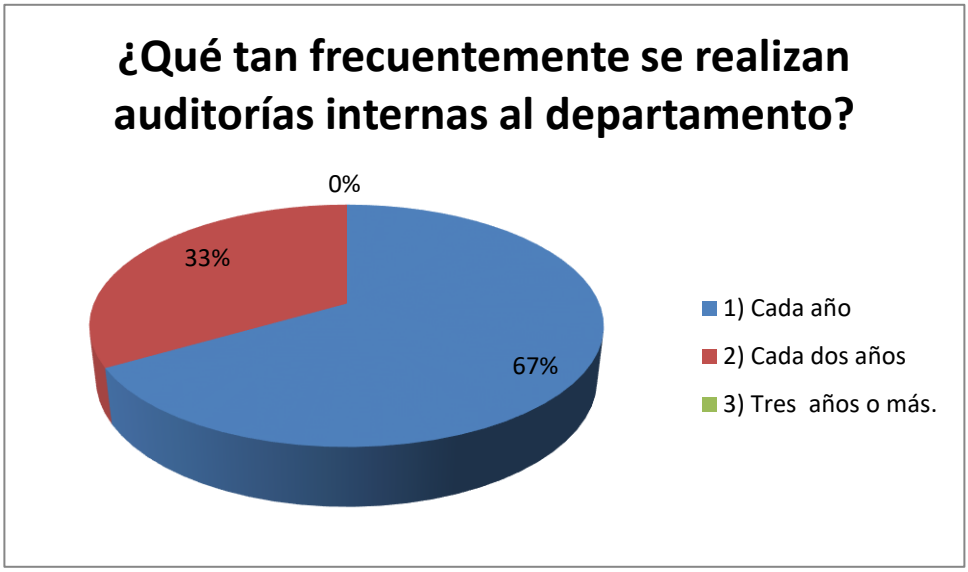
Análisis:

En el ámbito de conocimiento de los auditores en las buenas prácticas deben conocer acerca de la aplicación de programas que les ayuden a evaluar al área de informática.

Al observar los resultados obtenidos con los auditores encuestados se puede visualizar que el 81% de estos auditores no realizan auditorías al departamento de informática por falta de programas, interés por porte de la administración, entre otras causas; y solo un 19% respondió que realiza auditorías a esta área.

16. ¿Qué tan frecuentemente se realizan auditorías internas al departamento?

Objetivo: Conocer que tan frecuentemente se realizar auditorías internas al departamento de Informática.



Alternativa	Fr.	Fr. %
1) Cada año	2	67%
2) Cada dos años	1	33%
3) Tres años o más.	0	0%
	3	100%

Análisis:

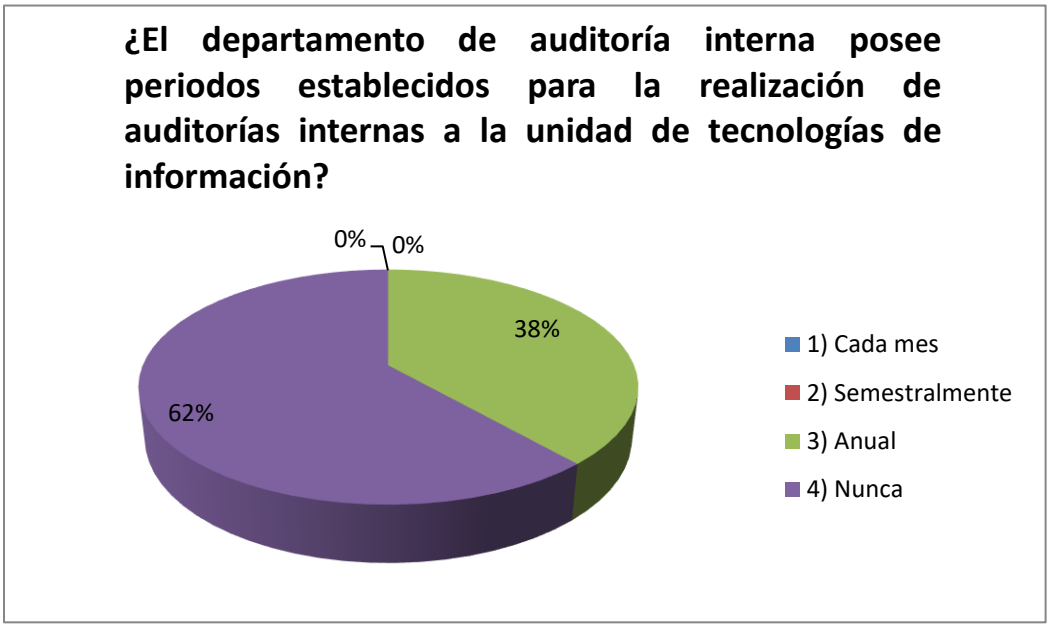
Con el conocimiento de buenas prácticas, los auditores cuentan con las herramientas necesarias para realizar un seguimiento de las auditorías en los distintos departamentos de las empresas.

El realizar auditorías a las diferentes áreas de la empresa es muy importante para verificar el adecuado funcionamiento de cada una de estas áreas, al encuestar a los auditores la frecuencia con la que realizan auditorías al área de T.I, se pudo observar que en su mayoría los auditores se abstuvieron a responder la pregunta, mostrando así que en su mayoría los auditores dejan de lado la evaluación a dicho departamento.

En los resultados obtenidos se pudo obtener que solo un 19% respondió a la interrogante, de los cuales un 13% auditores realizan auditorías anual mente y un 6% realiza auditorías cada dos años; mientras que un 81% se abstuvo a contestar la pregunta.

17. ¿El departamento de auditoría interna posee periodos establecidos para la realización de auditorías internas a la unidad de tecnologías de información?

Objetivo: Conocer el periodo sobre el cual se realizan evaluaciones al departamento de tecnologías de investigación.



Alternativa	Fr.	Fr. %
1) Cada mes	0	0%
2) Semestralmente	0	0%
3) Anual	5	38%
4) Nunca	8	62%
	13	100%

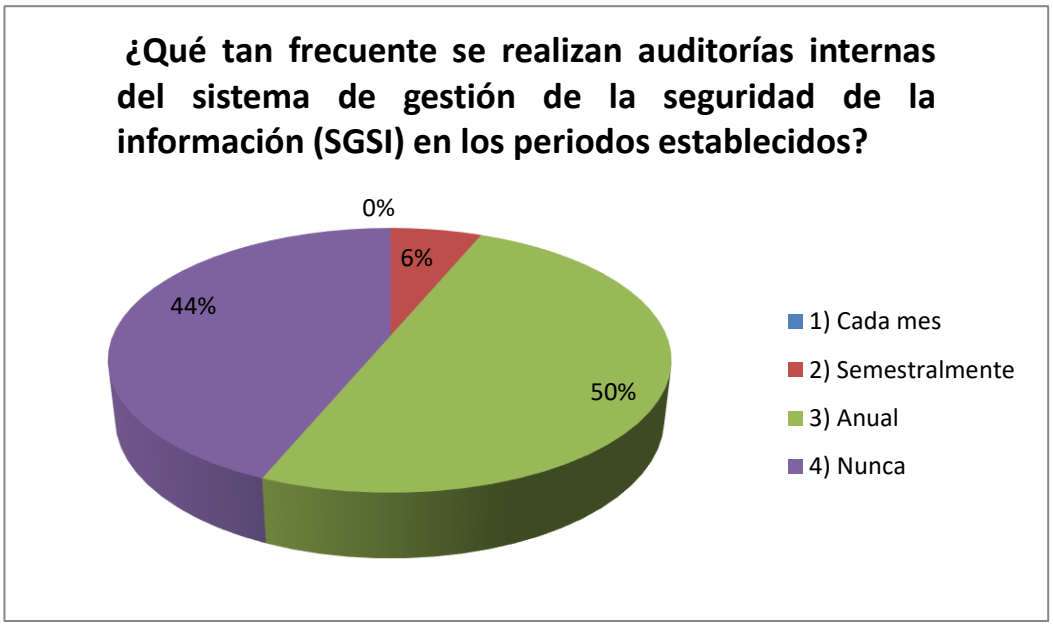
Análisis:

El cuidado de los activos tecnológicos que posee la empresa es uno de los aspectos que el departamento de auditoría interna debiera verificar, debido a la importancia que representa este activo al momento de administrar los créditos otorgados y la información que se maneja de los clientes.

En los resultados obtenidos con los encuestados se pudo observar que el 50% no posee periodos establecidos para realizar auditorías al departamento de T.I.; así mismo un 19% se abstuvo de responder lo cual indica que tampoco poseen periodos para evaluar a dicha área y solo un 31% cuenta con periodos establecidos para evaluar a dicha área los cuales se realizan anualmente.

18. ¿Qué tan frecuente se realizan auditorías internas del sistema de gestión de la seguridad de la información (SGSI) en los periodos establecidos?

Objetivo: Verificar si el departamento de auditoría interna evalúa el sistema de gestión de la seguridad de la información.



Alternativa	Fr.	Fr. %
1) Cada mes	0	0%
2) Semestralmente	1	6%
3) Anual	8	50%
4) Nunca	7	44%
	16	100%

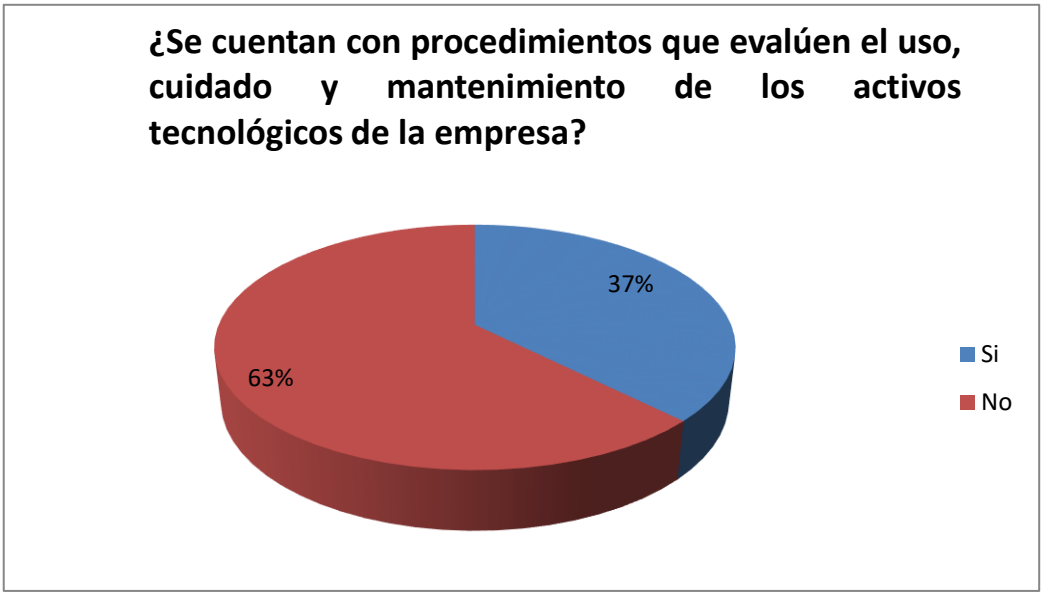
Análisis:

Los auditores deben poseer conocimientos en distintas áreas debido a la complejidad que cada una posee, uno de los conocimientos que se requieren al evaluar al departamento de T.I. son en la determinación de los riesgos que conlleva esta área por la vulnerabilidad de la tecnologías cambiantes y amenazas que existen en la web.

Los resultados obtenidos a través de la investigación arrojan resultados en los cuales se puede evidenciar que en su mayoría los auditores realizan en la seguridad de información en periodos anuales arrojando un porcentaje del 50%, pero también se observa que de igual manera un 44% nunca realiza una auditoría de este tipo y solo un 6% realiza auditorías de este tipo semestralmente.

19. ¿Se cuentan con procedimientos que evalúen el uso, cuidado y mantenimiento de los activos tecnológicos de la empresa?

Objetivo: Verificar si la unidad de auditoría interna cuenta con programas para la evaluación del uso, cuidado y mantenimiento de los activos tecnológicos de la entidad.



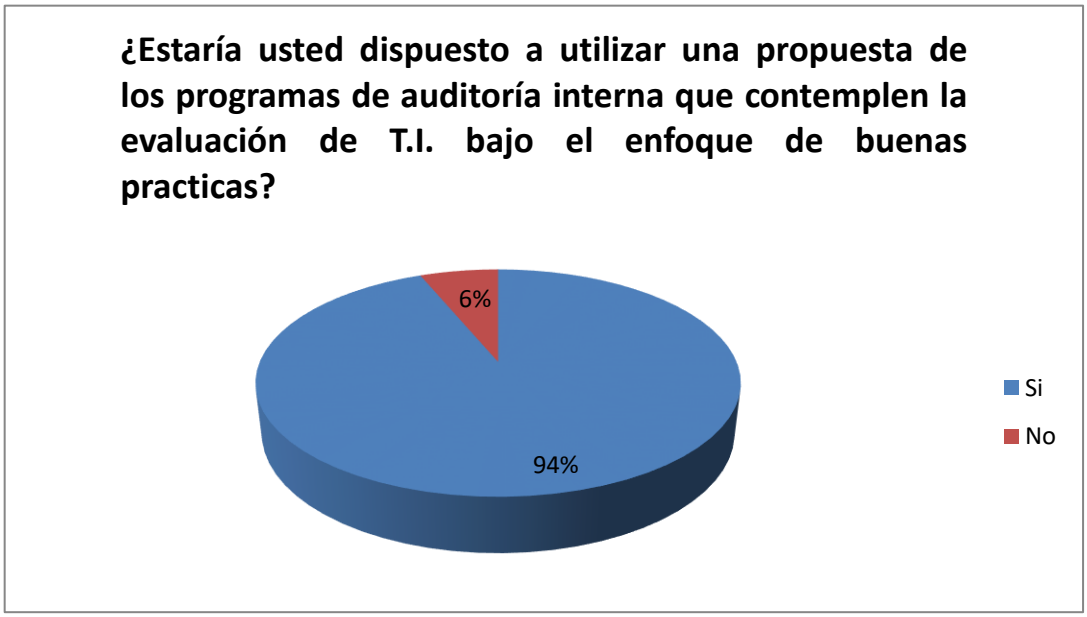
Alternativa	Fr.	Fr. %
Si	6	38%
No	10	63%
	16	100%

Análisis:
Uno de los cuidados que se deben poseer en el área de informática para resguardar la información con que se cuenta es el acceso a los sistemas por parte de los empleados, el departamento de auditoría debe evaluar los accesos y cuidados de los equipos tecnológicos con que cuenta el área de T.I.

El 63% de los auditores afirmaron que no poseen procedimientos que les ayuden a evaluar al departamento de informática en las empresas, dificultando esto la evaluación de dicha área; así mismo un 38% respondió que cuentan con programas para evaluar el área, sin embargo los mismos no son aplicados, ya que en relación a la interrogante N° 15 se estableció que no se realizan auditorías al departamento de T.I.

20. ¿Estaría usted dispuesto a utilizar una propuesta de los programas de auditoría interna que contemplen la evaluación de T.I. bajo el enfoque de buenas prácticas?

Objetivo: Determinar si el departamento de auditoría interna se encuentra interesado en poner en práctica los programas que se realizaran.



Alternativa	Fr.	Fr. %
Si	15	94%
No	1	6%
	16	100%

Análisis:

Los auditores necesitan herramientas que los ayuden a realizar de forma óptima sus labores diarias, es por eso que se ven en la necesidad de contar con procedimientos que ayuden a evaluar de forma adecuada al departamento de informática de la empresas, así también evaluar el riesgo y vulnerabilidades que este mismo posee con el crecimiento constante de la tecnología y el alto grado de amenazas que surgen día con día.

En los resultados obtenidos con la encuesta se pudo obtener que un 94% de la población encuestada se encuentra interesada en la propuesta de programas para evaluar al departamento de T.I., así mismo estarían dispuestos a utilizarlas en sus evaluaciones y solo un 6% respondió que no se encuentra interesado en dichos programas.

Anexo 3. MAPA DE CALOR

		PROBABILIDAD		
		1	**2**	**3**
IMPACTO		**BAJO**	**MEDIO**	**ALTO**
CALIFICACION		NO SE ESPERA QUE OCURRA	PUEDE OCURIR ALGUNAS VECES	SE ESPERA QUE OCURRA EN TODA LAS CIRCUNSTANCIAS
3	ALTO		b, c, d.	a
2	MEDIO		e, f	
1	BAJO		g	