ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

ESCUELA DE CONTABILIDAD Y AUDITORÍA

CARRERA DE INGENIERÍA EN CONTABILIDAD Y AUDITORÍA

TESIS DE GRADO PREVIA A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERA EN CONTABILIDAD Y AUDITORÍA C.P.A.

TEMA:

"AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS INFORMÁTICOS A LA EMPRESA SUMATEX, DE LA CIUDAD DE RIOBAMBA, PROVINCIA DE CHIMBORAZO POR EL PERIODO 2012".

SANDRA CAROLINA VALDIVIEZO CRIZÓN

Riobamba - Ecuador

2014

CERTIFICACIÓN DEL TRIBUNAL

Certificamos que el presente trabajo, "AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS INFORMÁTICOS A LA EMPRESA SUMATEX, DE LA CIUDAD DE RIOBAMBA, PROVINCIA DE CHIMBORAZO POR EL PERIODO 2012" ha sido revisado en su totalidad quedando autorizada su presentación.

Ing. MsC. Napoleón Cadena Oleas.	Ing. MsC. (a) Jimena Viteri Ojeda.
DIRECTOR DE TESIS	**MIEMBRO DEL TRIBUNAL**

CERTIFICADO DE AUTORÍA

Las ideas expuestas en el presente trabajo de investigación y que aparecen como propias es responsabilidad absoluta de la autora y de los autores descritos en la respectiva bibliografía.

SANDRA CAROLINA VALDIVIEZO CRIZÓN

DEDICATORIA

Este trabajo lo dedico primeramente a Dios como símbolo de agradecimiento por la infinita ayuda que me da, la sabiduría que me brinda en el transcurso de mi vida, mi profesión y hasta la culminación de un sueño importante; a Mis padres por su incondicional apoyo, a mi hermano por su valiosa compañía.

A mi hija Emily y a mi esposo Klever que son mi razón para luchar y seguir adelante, dando lo mejor de mí para ser una buena madre, esposa, profesional, hija, servidora y ejemplo para mi hija.

Sandra Carolina Valdiviezo Crizón.

AGRADECIMIENTO

Agradezco primero a Dios por guiar mi camino, llenarme de sabiduría, entendimiento, salud y vida para continuar y cumplir con mis metas de llegar a ser en la vida una persona digna del orgullo de mis padres, de la admiración de mi familia, del ejemplo para mi hija y de ayuda a la sociedad.

A mis padres: Fausto Valdiviezo, María Elena Crizón, a mi hermano Cristian por ser mi refugio familiar, por su ayuda, apoyo y comprensión en todo lo que he realizado en la vida y sobre todo en la culminación de mi profesión sin esperar nada a cambio con ejemplo de lucha, perseverancia, responsabilidad y humildad.

A mi esposo y mi hija que ahora son mi familia por estar conmigo en toda circunstancia brindándome amor, comprensión, y amistad, porque gracias a ellos he logrado culminar con mi carrera profesional, sembrando en mí las ganas de salir adelante.

A todos mis maestros que con sus amplios conocimientos me han colmado de sabiduría y valores éticos necesarios para ser útil en la sociedad, sin dejar de ser amigos, compañeros y padres en la Institución educativa que ha sido durante este tiempo mi segundo hogar y del cual me voy llevando gratos recuerdos de mi vida.

A mis amigas que con su carisma, amistad y confianza han sido mi ayuda, compañía y oído ante los momentos de disgustos y alegrías, caminando juntas hasta la culminación de nuestras carreras y a pesar de las dificultades hemos permanecido juntas.

Al personal y dirección de SUMATEX por brindarme el apoyo y apertura en su empresa para realizar mi trabajo de tesis, colaborando con responsabilidad, integridad y profesionalismo del cual los caracteriza a cada uno de ellos.

Un amplio, sincero e infinito agradecimiento a los Ingenieros Napoleón Cadena, Jimena Viteri y Lenin Gaibor que con su colaboración oportuna y pertinente han logrado que cumpla con mi sueño de ser profesional.

Sandra Carolina Valdiviezo Crizón

ÍNDICE DE CONTENIDO

ÍNDICE DE ILUSTRACIONES

Nº **DESCRIPCIÓN** **PÁGINA**

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

La presente Auditoría de Seguridad Física y Lógica de Sistemas Informáticos a la empresa SUMATEX de la ciudad de Riobamba, período 2012, se realizó con el objetivo de evaluar el grado de seguridad en estos dos aspectos fundamentales para los sistemas de información de la organización, ya que en la actualidad no se cuenta con las medidas necesarias para garantizar el salvaguardo de los sistemas y equipos, lo cual es de suma importancia para estar a la par de las innovaciones tecnológicas y la conservación de la información.

Se hizo la evaluación y análisis de la seguridad de los sistemas informáticos de SUMATEX, aplicando la metodología COSO II en lo referente a las pautas de control interno, lo cual proporcionó los elementos necesarios para finalmente emitir un informe que permita mejorar la integridad, confiabilidad y confidencialidad en el manejo de los equipos y de la información que son aspectos esenciales para una mejor toma de decisiones que incluso permitan la optimización de los procesos.

Actualmente SUMATEX no cuenta con una adecuada implementación de controles y mecanismos que permitan minimizar los riesgos detectados en el presente estudio, por lo tanto se recomienda implementar medidas de control interno que forman parte del informe final entregado a la dirección de la empresa.

ABSTRACT

This investigation was carried out the physical and logical security audit of information system at enterprise SUMATEX from Riobamba city, period 2012. It was made for evaluating security grade on these two fundamental aspects for systems of information to the organization, since in nowadays do not count with necessary steps in order to guarantee the safeguarded systems and equipment, which are very important to treat the couple of technological innovations and information conservation.

It made evaluation and analysis of security systems informatics at SUMATEX, applying the methodology COSO II guidelines regarding internal control, which provides the necessary elements to finally issue a report that will improve the integrity, reliability and confidentiality on handling of equipment and information that are essential to making better choices that even allow optimization of processes.

This enterprise does not have a suitable implementation of controls and mechanisms to minimize the risks identified in the present study, therefore it is recommended to implement internal control measures that are part of final repor.

INTRODUCCIÓN

La Auditoría Informática aparece a finales del siglo XX, dado que los sistemas informáticos se han constituido en las herramientas más poderosas para materializar uno de los conceptos más necesarios para toda empresa, cualquiera que sea su índole.

La informática esta hoy en día considerada como una herramienta fundamental de la gestión integral de las organizaciones, por lo que las normas y estándares propios de la informática deben ser asumidas con responsabilidad e incluirlas en la gestión empresarial.

De esta necesidad nace la auditoría de seguridad informática, ya que la gestión informática abarca no solamente el manejo de los procesos informáticos, sino la seguridad que se le da a los mismos para salvaguardar la información empresarial contenida en dichos recursos, aclarando que no siempre la informática es gestionada propiamente por la empresa, pero si ayuda a la toma de decisiones que conduzcan a la eficiencia y eficacia de los manejos de sistemas, paquetes y equipos informáticos; por ende, la aplicación de una Auditoría de seguridad Informática es de singular importancia para el buen funcionamiento de las empresas.

La auditoría de seguridad física y lógica de sistemas informáticos consiste en la aplicación de barreras físicas, software´s de protección y procedimientos de control como medidas de prevención y contramedidas ante posibles amenazas de pirateo o hackeo de información.

Desgraciadamente, la seguridad lógica es un aspecto olvidado con demasiada frecuencia a la hora de hablar de seguridad informática en general; en muchas organizaciones se suele tomar medidas para prevenir y detectar accesos físicos no autorizados o atentados a los recursos informáticos, pero rara vez para prevenir la acción de un atacante que intente acceder a la información confidencial contenida en el software de los equipos, sea de manera directa o indirecta.

El presente trabajo de tesis proporciona un amplio panorama de lo que es la aplicación y ejecución de una auditoría de seguridad física y lógica de sistemas informáticos, el que a su vez aporta de manera directa a la empresa SUMATEX con medidas de prevención y control que salvaguarden los recursos informáticos, optimicen su utilización, eficiencia, eficacia y propicien el desarrollo ideal de los sistemas de información.

CAPÍTULO I

1. PROBLEMA

SUMATEX tiene a su disposición el manejo de equipos y sistemas informáticos que resultan muy importantes para el desarrollo de las actividades, el cumplimiento de los objetivos y metas empresariales que se han planteado; equipos y sistemas que necesitan de medidas de control, seguridad, protección y resguardo continuo, eficiente y suficiente.

La empresa cuenta con un Sistema informático (SSiAM) que le permite realizar de una manera ágil y sencilla las tareas más importantes de su giro empresarial o negocio, sobre el cual necesita mantener un mejor control en el flujo de la Información, esto es: Inventarios, Facturaciones, Cuentas por Cobrar, Cuentas Pagar, Bancos y Contabilidad.

El SSiAM es un Software de fácil uso, pues si una persona ha realizado una factura a lápiz y papel, entonces con el SSiAM puede hacerlo electrónicamente; no necesita ser especialista en computación ni tener altos conocimientos contables para obtener los resultados deseados; sin embargo, a pesar de las ventajas que posee este sistema, la información con la que cuenta la empresa se expone a riesgos muy elevados a nivel informático, ya que no posee los soportes necesarios, ni la protección suficiente para salvaguardar la información de la Empresa.

Asimismo, el cuidado físico de los equipos es casi nulo, lo que indica que es propenso a daños severos, pérdidas significativas e incluso posibles plagios de información que vendrían de la mano con el posible robo de los equipos.

Por otra parte, no se mantiene una cultura de orden y protección a la información financiera informática, ya que no se sabe con exactitud la ubicación de datos históricos en forma de datos informáticos, más allá de que el sistema no contiene la información completa de las existencias totales de la empresa.

Finalmente, las protecciones físicas y lógicas son escazas, solo mantienen medidas básicas pero no son suficientes para brindar confianza en el manejo de los mismos.

1.1 ANTECEDENTES DEL PROBLEMA

1.1.1 Planteamiento del Problema

SUMATEX se inició el 3 de septiembre de 1986. Estableciéndose legalmente en la ciudad de Riobamba en el año 2007, teniendo como principal actividad comercial la fabricación de ropa deportiva, ropa blanca, prendas de vestir para dormir, trabajo, uniformes, y la comercialización de las mismas a nivel local y nacional.

SUMATEX mantiene un registro continuo de las operaciones contables y de control de inventarios a través de programas informáticos muy poco seguros, los cuales resultan ser un posible blanco fácil para el espionaje, perdidas de información, fraudes, errores, alteraciones, riesgos que deben ser considerados en la toma de decisiones.

El avance de la informática, los sistemas, las telecomunicaciones, y otras aplicaciones de tecnología, han hecho que la empresa SUMATEX tenga que adaptarse rápidamente a los cambios en todos los sentidos, en especial en el giro del negocio, el cual está íntimamente relacionado con la tecnología de la información en el desarrollo de los diferentes procesos empresariales.

1.1.2 Formulación del Problema

¿Cuál es el grado de seguridad, los niveles de confianza y de riesgo que la empresa SUMATEX mantiene en el manejo de las tecnologías de la información?

1.1.3 Delimitación del Problema

Ubicación del problema por su:

- Objeto de Estudio: Tecnologías de Información SSiAM utilizado en la empresa SUMATEX.
- Campo de acción: Análisis de la Seguridad Física y Lógica.
- Espacio y tiempo: Departamento de Sistemas Informáticos, contables, directivas, ventas y bodegas de SUMATEX, durante el período 2012.

1.2 OBJETIVOS

1.2.1 Objetivo General

Realizar una Auditoría de Seguridad Física y Lógica de los Sistemas Informáticos a la Empresa SUMATEX, de la ciudad de Riobamba, provincia de Chimborazo por el período 2012.

1.2.2 Objetivos Específicos

- Evaluar y analizar el manejo y situación actual de los Sistemas de Información de SUMATEX, enfocándose en el control tecnológico de información.
- Aplicar el estándar COSO (Committee of Sponsoring Organizations) elaborado por Treadway Commission, EE.UU. 1.992, referido a pautas de control interno en la evaluación y desarrollo de la auditoría de seguridad física y lógica de tecnologías de información en SUMATEX.
- Emitir un informe que permita otorgar una mayor integridad, confidencialidad y confiabilidad de la información para la mejor toma de decisiones, que ayude a la ejecución optima de los procesos de SUMATEX.

1.3 JUSTIFICACIÓN

El desarrollo tecnológico que enfrenta la empresa SUMATEX, con el manejo de diversos sistemas de información y automatización en sus procesos, necesita corregir fallas, ejecutar procesos de calidad y, entregarlos en el momento oportuno; para esto es necesario la aplicación de una Auditoría de Seguridad Física y Lógica de Sistemas Informáticos la que proponga recomendaciones efectivas, para minimizar riesgos y mejorar el empleo de la tecnología de información en la organización.

La evaluación de los sistemas de información, deberá cubrir aspectos de planificación, organización, dirección y control de los procesos, ejecución de proyectos, seguridades, equipos, redes y comunicaciones, todo con el objeto de determinar los riesgos a los que se encuentra expuesta SUMATEX y recomendar procedimientos que permitan minimizarlos o eliminarlos.

Como parte del sistema de administración de SUMATEX, se hace evidente la necesidad de evaluar y valorar el uso de las TIC´s, para de esta manera, justificar su costo y determinar medidas que permitan su racional aplicación, eficiencia y efectividad.

Esto se dirige a evaluar los métodos y procedimientos de uso de los sistemas informáticos de la empresa, con el propósito de determinar si su diseño y aplicación son correctos; y comprobar el sistema de procesamiento de información como parte de la evaluación de control interno; así como para identificar aspectos susceptibles de mejorarse.

La Auditoría de Sistemas Informáticos determinará si las Tecnologías de la Información salvaguardan los activos, mantienen la integridad de los datos, llevan a cabo eficazmente los objetivos de la organización, utilizan eficientemente los recursos y cumplen con las leyes y regulaciones establecidas; para así dar la seguridad de que el manejo de la empresa es acorde a los objetivos empresariales establecidos.

Finalmente determinaremos la confiabilidad y validez de la información, efectividad de los controles ya existentes, y la eficiencia de la información.

CAPÍTULO II

2. MARCO TEÓRICO

2.1 AUDITORÍA

En su estudio Alvin A. Arens (2005) concluye que:

Auditoría es la acumulación y evaluación de la evidencia basada en información para determinar y reportar sobre el grado de correspondencia entre la información y los criterios establecidos. La auditoría debe realizarla una persona independiente y competente. (p.5)

La evidencia es cualquier tipo de datos que utiliza el auditor para determinar si la información que está auditando ha sido declarada de acuerdo con el criterio establecido. La evidencia asume varias formas diferentes entre ellas:

- Testimonio oral de auditor (cliente)
- Comunicación por escrito con las partes externas.
- Observaciones por parte del auditor.
- Datos electrónicos sobre las transacciones.

Para satisfacer el propósito de la auditoría, quienes la lleven a cabo deben obtener calidad y volumen suficientes de evidencia. Los auditores deben determinar los tipos y cantidad de evidencia necesaria y evaluar si la información corresponde al criterio establecido. Ésta es una parte crítica de cada auditoría y el objeto principal de este libro. (p. 5)

En su estudio Walter G., Richard E. y William C. (1988) concluyen que:
La auditoría podrá definirse como:
Un proceso sistemático para obtener y evaluar evidencia de una manera objetiva respecto de las afirmaciones concernientes a actos económicos y eventos para determinar el grado de correspondencia entre estas afirmaciones y criterios establecidos y comunicar los resultados a los usuarios interesados. (p.22)

En su estudio Mario G. Piattini y Emilio P. (2001) concluyen que:
Conceptualmente la auditoría, toda y cualquier auditoría, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.(p. 4)

Por lo anterior, se concluye que:

La auditoría es proceso de análisis y verificación de la información en cumplimiento a los criterios establecidos; basados en evidencia real, suficiente y competente que permita llegar a una conclusión y opinión clara del cumplimiento que se está dando a los objetivos frente a lo que se busca cumplir en la organización.

2.2 CLASES DE AUDITORÍA

El objeto sometido a estudio, sea cual sea su soporte, y la finalidad con que se realiza el estudio, definen el tipo de auditoría de que se trata. A título ilustrativo podríamos enumerar entre otras: (p.4)

Tabla Nº 1

Clases de Auditoría

Clase	Contenido	Objeto	Finalidad
Financiera	Opinión	Cuentas Anuales	Presentan realidad
Informática	Opinión	Sistemas de aplicación, recursos informáticos, planes de contingencia, etc.	Operatividad eficiente y según normas establecidas.
Gestión	Opinión	Dirección	Eficacia, eficiencia, economicidad.
Cumplimiento	Opinión	Normas establecidas	Las operaciones se adecuan a estas normas.

2.3 TIPOS DE AUDITORÍA

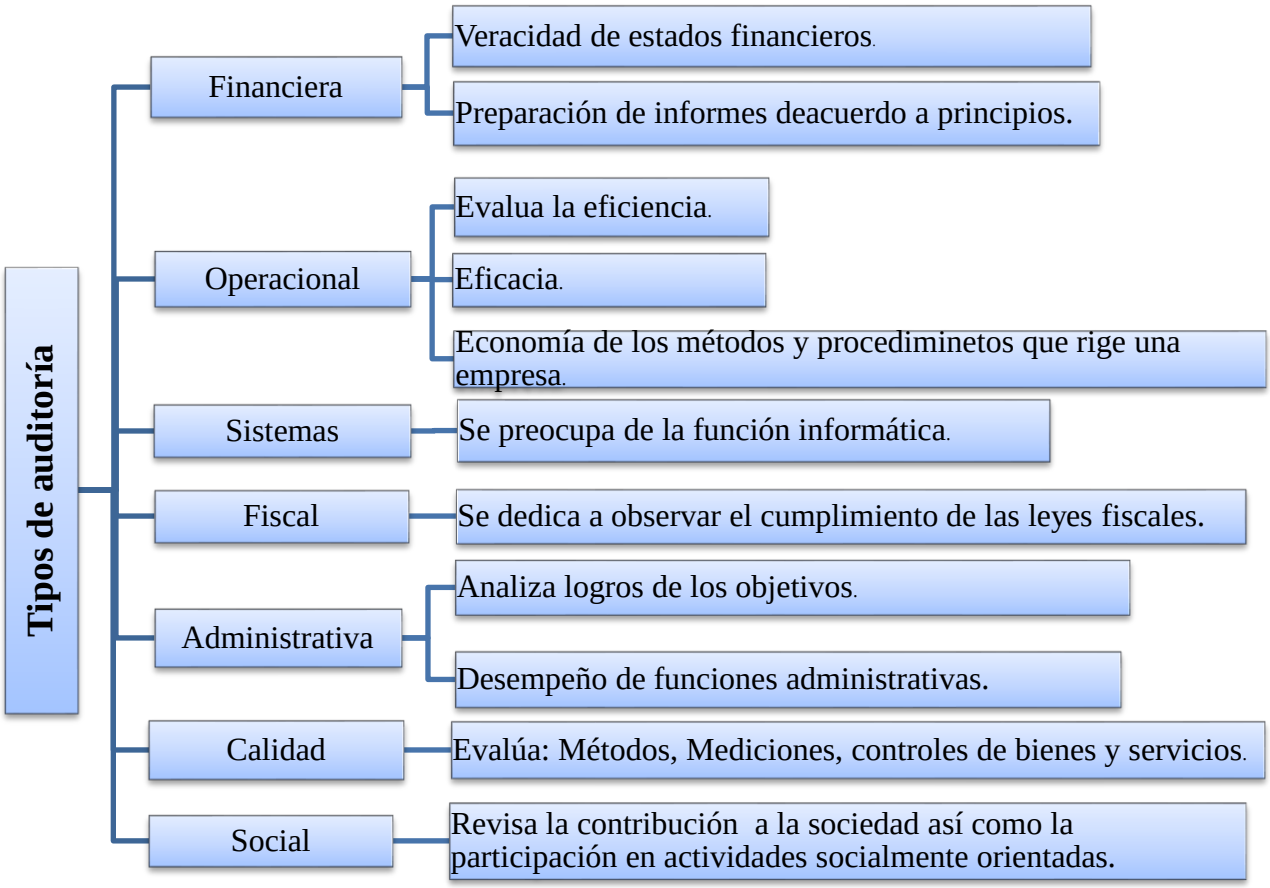
Según estudios realizados por MBA Alice Naranjo (año No Identificado), recuperado de: http://anaranjo.galeon.com/tipos_audi.htm

Existen algunos tipos de Auditoría entre las que la Auditoría de Sistemas integra un mundo paralelo pero diferente y peculiar, resaltando su enfoque a la función informática. Es necesario recalcar como análisis de este cuadro que Auditoría de Sistemas no es lo mismo que Auditoría Financiera.

Entre los principales enfoques de Auditoría, tenemos los siguientes:

Ilustración N° 1:

Tipos de Auditoría



Fuente: http://anaranjo.galeon.com/tipos_audi.htm

Según lo analizado anteriormente se considera que:

La auditoría es muy importante en todos sus ámbitos de aplicación cualquiera que sea éste; al igual que el área de estudios al que se quiera aplicar, de donde a la vez nace la importancia de la aplicación de auditorías informáticas en las empresas y sobre todo la seguridad física y lógica de sistemas informáticos.

2.4. SISTEMA DE CONTROL INTERNO INFORMÁTICO

Según los estudios de Mario G. Piattini (2001) describen:

Se puede definir el control interno como "cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos".

Históricamente, los objetivos de los controles informáticos se han clasificado con las siguientes categorías:

- *Controles preventivos:* para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.

- *Controles detectivos:* cuando fallan los preventivos para tratar de controlar cuanto antes el evento. Por ejemplo, el registro de intentos de accesos no autorizados, el registro de la actividad diaria para detectar errores u omisiones, etc.

- *Controles correctivos:* facilitan la vuelta a la normalidad cuando producido incidencias. Por ejemplo, la recuperación de un archivo de datos a partir de las copias de seguridad. (p.31)

Por lo anterior se considera que:

Los controles son todas aquellas medidas que se toman para contrarrestar los riesgos sean estos detectados antes, durante y después de haberse presentado los mismos; para de esta manera lograr el normal y eficiente cumplimiento de los objetivos establecidos por las organizaciones.

Según estudios de George Beekman (año no identificado)

2.5 AUDITORÍA DE SISTEMAS O INFORMÁTICA

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables para el procesamiento de datos en sistemas informáticos.

Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Según los estudios de Mario G. Piattini (2001) describe:

La Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva acabo eficazmente los fines de la organización y utiliza eficientemente los recursos. De este modo la auditoría informática confirma la consecución de los objetivos tradicionales de la auditoría:

- Objetivos de protección de activos e integridad de datos.
- Objetivos de gestión que abarcan, no solamente los de protección operacional sino también los de eficacia y eficiencia.

Por lo anterior se considera que:

La Auditoría de seguridad informática es la encargada de evaluar si el funcionamiento de los sistemas y equipos informáticos es el correcto y si la información confidencial es asegurada a manera que esta sea de acceso único del personal acreditado y legalmente autorizado en sus funciones, aportando de esta manera con una opinión concreta y concisa que guie al cumplimiento de los objetivos empresariales.

2.6 SEGURIDAD INFORMÁTICA FÍSICA Y LÓGICA

Para lograr sus objetivos la seguridad informática se fundamenta en principios, que debe cumplir todo sistema informático.

Recuperado de: http://alarcos.inf-cr.uclm.es/doc/calidadSI/CSI-Tema4.pdf

Seguridad es la capacidad de un producto software de proteger los datos y la información para que personas no autorizadas no puedan leerlos o modificarlos, y que el acceso no sea denegado a personal autorizado (ISO/IEC, 1999b)

Confidencialidad: Prevenir / detectar / impedir el descubrimiento de información. En general Confidencialidad se refiere a la protección de datos implicados en entornos altamente protegidos, como entornos militares, comerciales, etc. Privacidad se refiere a información sobre individuos. En la mayoría de los países la Privacidad está protegida por las leyes.

Integridad: Prevenir / detectar / impedir la modificación inadecuada de información. Por ejemplo en un entorno militar, el mando responsable de un misil no debe ser modificado inadecuadamente. En un entorno comercial, la integridad de los datos es especialmente relevante, puesto que el éxito de una organización depende de lo correctas que son las operaciones que se llevan a cabo y la coherencia en los datos.

Disponibilidad: prevenir / detectar / impedir la denegación inadecuada del acceso a servicios ofrecidos por el sistema. Por ejemplo, en un entorno militar, cuando el mando correspondiente da la orden de lanzar el misil, el misil es disparado. En entornos comerciales, las órdenes de pago deben ser hechas en el momento. (p. 7 - 8 - 9 - 10)

Según los estudios de Royal P. Fisher (1988) describe:

Integridad: Un sistema debería hacer sólo lo que se supone que debe hacer y nada más; se realiza de acuerdo con un conjunto proyectado de especificaciones incluso cuando falla. Posee los elementos de información completa en su totalidad. Tal sistema tiene integridad. La propiedad de integridad prevee la capacidad para responder con una acción correctora.

Tal sistema reduce mucho el potencial para la exposición de información, y de este modo eleva el nivel de la seguridad de los datos.
(p.24)

Auditabilidad: Un sistema que es auditable permite a un inspector independiente verificar su actividad con facilidad relativa en cualquier momento. El sistema debe demostrar que está ejecutándose para las especificaciones, obedeciendo las respuestas de control, siendo utilizado como ha pensado hacerse y conforme con las normas de buena práctica. Para obtener este criterio, el sistema debería ser construido totalmente con componentes auditables.

Necesita ser modular en diseño cada módulo capaz de comunicar con otros sólo a través de un número limitado de interfaces determinadas realmente. Tal sistema tiene la aptitud para registrar todas las transacciones (demandas, sucesos, contenidos, estímulos, respuestas) en las interfaces. (p.25)

Controlabilidad: Un sistema que posee Controlabilidad permite a la dirección ejercer una influencia ordenada o restringida sobre su uso, comportamiento o contenido. Esta propiedad limita la capacidad de un sistema para pasar a otro que intente u ordene recursos entre dominios diferentes (por ejemplo, áreas de trabajo o esferas de influencia). Por ejemplo, yo puedo ser capaz de emitir cargas a una cuenta de gastos del negocio, pero no aprobarlas. Además, se me puede permitir emitir los costes sólo para tipos particulares de cargos asociados con mi departamento.

Para alcanzar este control, cada módulo auditable debe ser individualmente controlable. Esto implica que cada módulo controle su propio dominio, de modo que pasan a otros módulos sólo aquellas acciones determinadas. (p.26)

Por lo anterior se considera que:

Una seguridad de sistemas informáticos deben fundamentarse en principios que permita tener un control adecuado sobre su manejo independiente, claro y conciso dispuesto a análisis y evaluaciones de auditoría y sobre todo controlable, de manera que pueden aplicarse medidas de precaución y cuidado de la información confidencial: y, de esta manera brindar seguridad en el manejo y uso de la información resguardando los activos de la organización.

Gestión del riesgo

Según los estudios de Gonzalo Álvarez M. y Pedro P. Pérez (2004) describe:

Resulta ilusorio creer que los riesgos pueden eliminarse por completo, en su lugar deben reducirse a niveles aceptables. La determinación de este nivel dependerá en gran medida de los objetivos concretos en la organización, del valor de sus activos, de su dimensión y presupuesto de seguridad. Lo más sorprendente es que ésta reducción del riesgo se puede conseguir con muy poco esfuerzo y una modesta inversión.

La seguridad de la información requiere un enfoque holístico, que implique la participación coordinada de tecnología, personas y operaciones. Su objeto no es conseguir sistemas 100% seguros, espejismo imposible de alcanzar, sino sistemas tan seguros como sea necesario para proteger los activos con un nivel que se corresponda con las expectativas. Recuerde:

El riesgo no puede eliminarse completamente, pero puede reducirse.

La seguridad de la información trata por tanto de proteger activos, tanto tangibles, como por ejemplo un disco duro o una base de datos con la información de clientes, como intangibles, como por ejemplo la reputación, la privacidad o el nombre de marca. Antes de lanzarse ciegamente a implantar medidas de seguridad que no se sabe muy bien qué es lo que van a proteger ni contra qué. Se debe realizar una labor precia de análisis:

- Identificar cuáles son los activos a proteger de la organización: ¿Qué activos son los más valiosos? ¿Cuál es su valor? ¿Cuánto cuesta reponerlos si se pierde o degradan? ¿Es posible reponerlos?

- Identificar las amenazas a que está expuestos los activos: ¿Cuáles son las amenazas naturales y humanas? ¿Qué agentes pueden realizar esas amenazas? ¿En qué circunstancias pueden producirse?

- Identificar los riesgos que suponen las amenazas para los activos: ¿Cuál es la probabilidad de que ocurra una amenaza? ¿Cuál es el coste tangible o intangible para la organización si la amenaza se materializa en un ataque?

- Identificar y evaluar el coste de las contramedidas a implantar para reducir o mitigar el riesgo: ¿De qué manera puede mitigarse el riesgo? ¿Cuánto cuesta implantar una contramedida? ¿Cuál es su eficacia? (p. 4 – 5)

Controles de seguridad de la información (p. 9)

Tabla Nº 2

Controles de seguridad informática

Control	Descripción	Ejemplos
Preventivo	Intenta evitar la ocurrencia de sucesos indeseados	Cortafuegos en el perímetro o filtrado de virus en la pasarela de correo
Detectivo	Intenta identificar sucesos indeseados después de que hayan ocurrido.	IDS de red o firmas de archivos para detectar cambios en el sistema de archivos
Disuasorio	Intenta disuadir a los individuos de violar intencionalmente las políticas o procedimientos de seguridad.	Amenaza de despido por violación de políticas o bloqueo de cuentas tras un determinado número de intentos de inicio de sesión fallidos.
Correctivo	Intenta remediar las circunstancias que permitieron la actividad ilegítima o devolver el sistema al estado anterior a la violación.	Reconfiguración automática de reglas del cortafuegos o eliminación de un virus y actualización de sus firmas.
Recuperativo	Intenta restaurar los recursos perdidos y ayudar a la organización a recuperarse de las pérdidas económicas causadas por la violación.	Copia de respaldo o planes de continuidad de negocio y de recuperación de desastres.

Fuente: Seguridad Informática para empresas y particulares. Gonzalo Álvarez M. y Pedro P. Pérez (2004)

Por lo anterior se considera que:

En una organización no podemos evitar los riegos de una manera total pero si se pueden prevenir y reducir de tal manera que cuide los activos de la empresa y aporte al cumplimiento de los objetivos, considerando que exista en medidas que se pueden aplicar de una manera fácil y sin inversiones exageradas o incomodas, más bien son medidas de evaluación, cuidado y prevención lo que a la vez su falta de aplicación y descuido pueden incurrir en pérdidas relevantes y representativas. Para evitar riesgos hace falta medidas para identificar las causas y fuentes de donde provienen dichos riesgos, poniendo en práctica controles preventivos, detectivos, disuasorios, correctivos y recuperativos.

Artículo recuperado de: http://www.monografías.com/trajajos11/metods/metods.shtml

2.7 RESTRICCIONES DE ACCESO FÍSICO Y LÓGICO A LOS SISTEMAS INFORMÁTICOS

Verificación Automática de Firmas (VAF): Usando emisiones acústicas toma datos del proceso dinámico de firmar o de escribir. La secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es único en cada individuo. El patrón contiene información extensa sobre la manera en que la escritura es ejecutada. El equipamiento de colección de firmas es inherentemente de bajo costo y robusto. Esencialmente, consta de un bloque de metal (o algún otro material con propiedades acústicas similares) y una computadora barata.

Sistema Biométrico: La Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas., La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas digitales y voz).

Huella Digital Basado en el principio de que no existen dos huellas dactilares iguales, este sistema viene siendo utilizado desde el siglo pasado con excelentes resultados. Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos, etc. (llamados minucias)

características y la posición relativa de cada una de ellas es lo analizado para establecer la identificación de una persona. Esta aceptado que dos personas no tienen más de ocho minucias iguales y cada una posee más de 30, lo que hace al método sumamente confiable.

Verificación de Voz: La dicción de una (o más) frase es grabada y en el acceso se compara la vos (entonación, diptongos, agudeza, etc.). Este sistema es muy sensible a factores externos como el ruido, el estado de ánimo y enfermedades de la persona, el envejecimiento, etc.

Verificación de Patrones Oculares: Estos modelos pueden estar basados en los patrones del iris o de la retina y hasta el momento son los considerados más efectivos (en 200 millones de personas la probabilidad de coincidencia es casi 0).

Contraseñas: Son las herramientas más utilizadas para restringir el acceso a los sistemas informáticos. Sin embargo, sólo son efectivas si se escogen con cuidado, la mayor parte de los usuarios de computadoras escogen contraseñas que son fáciles de adivinar: El nombre de la pareja, el de un hijo o el de una mascota, palabras relacionadas con trabajos o aficiones o caracteres consecutivos del teclado.

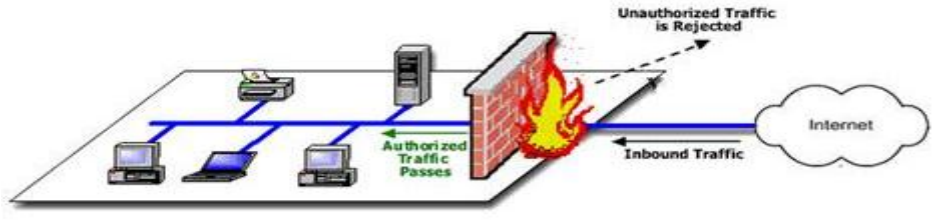
Según los estudios realizados por Álvaro Gómez V. (2013) concluye que:

Firewalls (cortafuegos): Es un dispositivo que realiza un filtrado de paquetes de datos a partir de unas reglas definitivas por el administrador de la red, teniendo en cuenta las direcciones IP fuente o destino (es decir, de qué ordenador provienen y a qué ordenador van dirigidos los paquetes de datos) y el servidor de red al que se corresponden.

El muro contrafuegos está constituido por un dispositivo hardware, es decir, por una máquina específicamente diseñada y construida para esta función, aunque también podría utilizarse un software que se instala en un ordenador conectado a la red de la organización. (p.127)

A continuación se puede observar el diseño del trabajo del firewalls tomado de diferente fuente conservando su interpretación.

Ilustración N° 2: Muro Cortafuegos



Fuente: http://www.monografias.com/trabajos82/la-seguridad-informatica/.shtml

Artículo recuperado de: http://www.monografías.com/trabajos11/métods/metods.shtml

Como puede observarse, el Muro Cortafuegos, sólo sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Tipos de Firewall

- Filtrado de Paquetes
- Proxy-Gateways de Aplicaciones
- Dual-Homed Host
- Screened Host
- Screened Subnet

Inspección de Paquetes: Este tipo de Firewalls se basa en el principio de que cada paquete que circula por la red es inspeccionado, así como también su procedencia y destino. Se aplican desde la capa de Red hasta la de Aplicaciones. Generalmente son instalados cuando se requiere seguridad sensible al contexto y en aplicaciones muy complejas.

Firewalls Personales: Estos Firewalls son aplicaciones disponibles para usuarios finales que desean conectarse a una red externa insegura y mantener su computadora a salvo de ataques que puedan ocasionarle desde un simple "cuelgue" o infección de virus hasta la pérdida de toda su información almacenada

Filtrado de paquetes: El filtrado de paquetes mediante puertos y protocolos permite establecer que servicios estarán disponibles al usuario y por cuales puertos. Se puede permitir navegar en la WWW (puerto 80 abierto) pero no acceder a la transferencia de archivos vía FTP (puerto 21 cerrado).

Debido a su funcionamiento y estructura basada en el filtrado de direcciones y puertos este tipo de Firewalls trabajan en los niveles de Transporte y de Red del Modelo OSI y están conectados a ambos perímetros (interior y exterior) de la red.

Proxy-Gateways de Aplicaciones: Para evitar las debilidades asociadas al filtrado de paquetes, los desarrolladores crearon software de aplicación encargados de filtrar las conexiones. Estas aplicaciones son conocidas como Servidores Proxy y la máquina donde se ejecuta recibe el nombre de Gateway de Aplicación o Bastion Host.

Ilustración N° 3: Proxy de aplicaciones.

Fuente: http://www.monografias.com/trabajos82/la-seguridad-informatica/.shtml

Dual-Homed Host: Son dispositivos que están conectados a ambos perímetros (interior y exterior) y no dejan pasar paquetes IP (como sucede en el caso del Filtrado de Paquetes), por lo que se dice que actúan con el "IP-Forwarding desactivado".
Un usuario interior que desee hacer uso de un servicio exterior, deberá conectarse primero al Firewall, donde el Proxy atenderá su petición, y en función de la configuración impuesta en dicho Firewall, se conectará al servicio exterior solicitado y hará de puente entre este y el usuario interior.

Es decir que se utilizan dos conexiones. Uno desde la máquina interior hasta el Firewall y el otro desde este hasta la máquina que albergue el servicio exterior.

Ilustración N° 4: Dual-Homed Host

Fuente: http://www.monografias.com/trabajos82/la-seguridad-informatica/.shtml

Screened Host: En este caso se combina un Router con un host bastión y el principal nivel de seguridad proviene del filtrado de paquetes. En el bastión, el único sistema accesible desde el exterior, se ejecuta el Proxy de aplicaciones y en el Choke se filtran los paquetes considerados peligrosos y sólo se permiten un número reducido de servicios.

Ilustración N° 5: Combinación Router con host bastión

Fuente: http://www.monografias.com/trabajos82/la-seguridad-informatica/.shtml

Screened Subnet: En este diseño se intenta aislar la máquina más atacada y vulnerable del Firewall, el Nodo Bastión. Para ello se establece una Zona Desmilitarizada (DMZ) de forma tal que sin un intruso accede a esta máquina no consiga el acceso total a la subred protegida.
En este esquema se utilizan dos Routers: uno exterior y otro interior. El Router exterior tiene la misión de bloquear el tráfico no deseado en ambos sentidos: hacia la red interna y hacia la red externa. El Router interior hace lo mismo con la red interna y la DMZ (zona entre el Router externo y el interno).

Ilustración N° 6: Zona Desmilitarizada

Fuente: http://www.monografias.com/trabajos82/la-seguridad-informatica/.shtml

Como puede apreciarse la Zona Desmilitarizada aísla físicamente los servicios internos, separándolos de los servicios públicos. Además, no existe una conexión directa entre la red interna y la externa.

Criptología: La encriptación como proceso forma parte de la criptología, ciencia que estudia los sistemas utilizados para ocultar información, La criptología es la ciencia que estudia la transformación de un determinado mensaje en un código de forma tal que a partir de dicho código solo algunas personas sean capaces de recuperar el mensaje original.

Métodos de Encriptación: Para poder encriptar un dato, se pueden utilizar tres procesos matemáticos diferentes. Los algoritmos HASH, los simétricos y los asimétricos.

Algoritmo HASH: Este algoritmo efectúa un cálculo matemático sobre los datos que constituyen el documento y da como resultado un número único llamado MAC. Un mismo documento dará siempre un mismo MAC.

Criptografía de Clave Secreta o Simétrica: Utilizan una clave con la cual se encripta y desencripta el documento. Todo documento encriptado con una clave, deberá des-encriptarse, en el proceso inverso, con la misma clave, es importante destacar que la clave debería viajar con los datos, lo que hace arriesgada la operación, imposible de utilizar en ambientes donde interactúan varios interlocutores.

Los Criptosistemas de clave secreta se caracterizan porque la clave de cifrado y del descifrado es el mismo, por tanto la robustez del algoritmo recae en mantener el secreto de la misma.

Algoritmos Asimétricos (RSA): Requieren dos claves, una privada (única y personal, solo conocida por su dueño) y la otra llamada pública, ambas relacionadas por una fórmula matemática compleja imposible de reproducir. El concepto de criptografía de clave pública fue introducido por Whitfield Diffie y Martin Hellman a fin de solucionar la distribución de claves secretas de los sistemas tradicionales, mediante un canal inseguro. El usuario, ingresando su PIN genera claves Públicas y Privadas necesarias

Firma Digital: La firma digital permite garantiza algunos conceptos de seguridad y son importantes al utilizar documentos en formato digital, tales como identidad o autenticidad,

integridad y no repudio. El modo de funcionamiento es similar a lo explicado para los algoritmos de encriptación, se utilizan también algoritmos de clave pública, aplicados en dos etapas.

Encriptar datos en un PDA: La importancia de tener nuestros datos a salvo de miradas extrañas o tener un mínimo de privacidad se ha convertido en un tema muy importante. Los PDA son muchas veces usados como pequeñas oficinas portátiles donde se guardan datos de gran valor y donde es de gran importancia tener estos datos protegidos. Muchos usuarios PDA por comodidad no protegen el acceso de inicio con una clave, imagínense en caso de pérdida del aparato o descuido poder dejar estos datos confidenciales en manos ajenas a las nuestras. Para solucionar este problema o tener cierto grado de seguridad, es muy importante poder encriptar nuestros datos.

Encriptación de Ficheros: Windows XP profesional nos da una alternativa para poder proteger estos datos y prevenir su pérdida. El Encripting File System (EFS) en el encargado de codificar los ficheros. Estos Ficheros solo se pueden leer cuando el usuario que los ha creado hace "logon" en su máquina (con lo cual, presumiblemente, nuestra password será una pasword robusta). De hecho, cualquiera que acceda a nuestra máquina, no tendrá nunca acceso a nuestros ficheros encriptados aunque sea un administrador del equipo.

Autenticación: Este proceso, es otro método para mantener una comunicación seguro entre ordenadores. La autenticación es usada para verificar que la información viene de una fuente de confianza. Básicamente, si la información es auténtica, sabes quién la ha creado y que no ha sido alterada. La encriptación y la autenticación, trabajan mano a mano para desarrollar un entorno seguro.

Hay varias maneras para autenticar a una persona o información en un ordenador:

- **Contraseñas:** El uso de un nombre de usuario y una contraseña provee el modo más común de autenticación. Esta información se introduce al arrancar el ordenador o acceder a una aplicación. Se hace una comprobación contra un fichero seguro para confirmar que coinciden, y si es así, se permite el acceso.

- **Tarjetas de acceso:** Estas tarjetas pueden ser sencillas como si de una tarjeta de crédito se tratara, poseyendo una banda magnética con la información de autenticación. Las hay más sofisticadas en las que se incluye un chip digital con esta información.

- **Firma digital:** Básicamente, es una manera de asegurar que un elemento electrónico (email, archivo de texto, etc.) es auténtico. Una de las formas más conocidas es DSS (Digital Signature Standard) la cual está basada en un tipo de encriptación de clave pública la cual usa DSA (Digital Signature Algorithm). El algoritmo DSA consiste en una clave privada, solo conocida por el que envía el documento (el firmante), y una clave pública. Si algo es cambiado en el documento después de haber puesto la firma digital, cambia el valor contra lo que la firma digital hace la comparación, invalidando la firma.

Antivirus: Los antivirus son herramientas simples; cuyo objetivo es detectar y eliminar virus informáticos. Nacieron durante la década de 1980.

Un virus informático ocupa una cantidad mínima de espacio en disco (el tamaño es vital para poder pasar desapercibido), se ejecuta sin conocimiento del usuario y se dedica a auto-replicarse, es decir, hace copias de sí mismo e infecta archivos, tablas de partición o sectores de arranque de los discos duros y disquetes para poder expandirse lo más rápidamente posible.

Básicamente, el propósito de un virus es provocar daño en el equipo infectado.
Normalmente un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados, en tiempo real. Es muy común que tengan componentes que revisen los adjuntos de los correos electrónicos salientes y entrantes, así como los scripts y programas que pueden ejecutarse en un navegador web (ActiveX, Java, JavaScript).

Los antivirus son esenciales en sistemas operativos cuya seguridad es baja, como Microsoft Windows, pero existen situaciones en las que es necesario instalarlos en sistemas más seguros, como Unix y similares.
Con tantos software malignos dando vuelta por internet, se hace necesario disponer de un buen antivirus que nos proteja continuamente.

Copias de Seguridad/Backups: Incluso el sistema de seguridad más sofisticado no puede garantizar al cien por ciento una protección completa de los datos. Un pico o una caída de tensión pueden limpiar en un instante hasta el dato más cuidadosamente guardado. Un UPS (Sistema de alimentación ininterrumpida) puede proteger a las computadoras contra la perdida de datos durante una caída de tensión, los más baratos pueden emplearse en las casas para apagones de corta duración. Los protectores de sobrecarga no sirven durante un apagón, pero si protegen los equipos contra los dañinos picos de tensión, evitando costosas reparaciones posteriores.

Por supuesto los desastres aparecen de formas muy diversas. Los sabotajes, los errores humanos, los fallos de la máquina, el fuego, las inundaciones, los rayos y los terremotos pueden dañar o destruir los datos de la computadora además del hardware.

Cualquier sistema de seguridad completo debe incluir un plan de recuperación en el caso de producirse un desastre. En mainframes y PC, lo mejor, además de ser lo más utilizado, es llevar a cabo copias de seguridad regulares.

Hacker: es una persona que sólo desea conocer el funcionamiento interno de los sistemas informáticos, ayudando a mejorarlos en el caso de que detecte fallos en su seguridad. Sin embargo, un 'hacker' deja de serlo cuando provoca daños y su acción es malintencionada: en ese momento pasa a ser un "cracker".

Para un 'hacker', el objetivo es saltar los sistemas de seguridad de los servidores de Internet para llegar hasta su interior, pero, una vez dentro, no causar ningún daño.

Cracker: Es cualquier persona que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

El cracker, es considerado un "vandálico virtual". Este utiliza sus conocimientos para invadir sistemas, descifrar claves y contraseñas de programas y algoritmos de encriptación, ya sea para poder correr juegos sin un CD-ROM, o generar una clave de registro falsa para un determinado programa, robar datos personales, etc.

Algunos tipos de crackers:

Crackers de sistemas: término designado a programadores que alteran el contenido de un determinado programa, por ejemplo, alterando fechas de expiración de un determinado programa para hacerlo funcionar como si se tratara de una copia legítima.

Crackers de Criptografía: término usado para aquellos que se dedican a la ruptura de criptografía (cracking codes)

Phreaker: cracker especializado en telefonía. Tiene conocimiento para hacer conexiones gratuitas, reprogramar centrales telefónicas, grabar conversaciones de otros teléfonos para luego poder escuchar la conversación en su propio teléfono, etc.

Cyberpunk: son los vándalos de páginas web o sistemas informatizados. Destruyen el trabajo ajeno.

Por lo anterior se considera que:

Al existir una variedad de métodos, sistemas y tipos de controles que se pueden aplicar en las organizaciones, hace que las empresas puedan evitar de cualquier manera la exposición de los datos y la información a los diferentes riesgos existentes en el medio informático, con tan solo realizar un análisis de las amenazas a los que se enfrentan y de las medidas que se pueden tomar para contrarrestarlos.

2.8 SISTEMA DE CONTROL INTERNO COSO

Estudiado y Recuperado de: http://www.pwc.com/cl/es/cursos/finanzas-y-analisis-cuantitativo/coso-ii-enfoque-para-administracion-corporativa-de-riesgos.jhtml

"Hace más de una década el Committee of Sponsoring Organizations of the Treadway Commission, conocido como COSO, publicó el Internal Control - Integrated Framework para facilitar a las empresas la evaluación y mejora de sus sistemas de control interno. Desde entonces ésta metodología se incorporó en las políticas, reglas y regulaciones y ha sido utilizada por muchas compañías para mejorar sus actividades de control hacia el logro de sus objetivos."

De lo anterior se considera que:

El sistema de control interno que manejan en las empresas es el único método que ayuda a las empresas a ejecutar sus operaciones de manera eficiente, que aporten al cumplimiento de los objetivos y conlleven al éxito empresarial.

Estudiado y Recuperado de: http://www.consejo.org.ar/comisiones/com_43/files/coso_2.pdf

"Control Interno es un proceso llevado a cabo por el Consejo de Administración, la Gerencia y otro personal de la Organización, diseñado para proporcionar una garantía razonable sobre el logro de objetivos relacionados con operaciones, reporte y cumplimiento."

Sin dejar de considerar que los usuarios externos son una fuente importante para el desarrollo de la empresa, pero debido al desconocimiento de estos componentes y la poca posibilidad de acercamiento hasta ellos, solo hemos considerado los usuarios internos. **(Anexo N° 2: Tabulación)**

Ilustración Nº 7 COSO

Fuente: http://www.consejo.org.ar/comisiones/com_43/files/coso_2.pdf

Ilustración Nº 8 Desarrollo de Componentes

Fuente: http://www.consejo.org.ar/comisiones/com_43/files/coso_2.pdf

Componentes COSO II

- Ambiente Interno
- Establecimiento de Objetivos
- Identificación del riesgo
- Evaluación del riesgo
- Respuesta al Riesgo
- Actividades de control
- Información y Comunicación
- Monitoreo

Componentes del Método COSO II los cuales fueron tomados en la aplicación de esta investigación de tesis, consecuentemente en la aplicación de Cuestionarios de Control Interno y análisis de áreas críticas.

CAPÍTULO III

3. MARCO METODOLÓGICO

La presente investigación está enmarcada dentro del paradigma crítico propuesto, por lo tanto tiene un enfoque cualitativo – cuantitativo, ya que se trabaja con sentido holístico y participativo considerando una realidad dinámica, pero al mismo tiempo está orientada a la consecución de resultados.

3.1 TIPOS DE INVESTIGACIÓN

3.1.1 TIPOS

La presente investigación abarca desde el nivel exploratorio hasta el nivel explicativo, pues se reconocen los componentes del problema, se establece las características de la realidad investigadas, el grado de relación que existe entre las causas y consecuencias del problema, llegando a la comprobación de la idea a defender.

3.1.2 MODALIDAD

En el desarrollo del proceso investigativo se empleó la investigación bibliográfica para la elaboración del marco teórico y la investigación de campo para la recolección de datos que sirvieron para la elaboración de la propuesta.

3.2 POBLACIÓN Y MUESTRA

El trabajo investigativo se realizó en las Oficinas principales de Dirección, Contabilidad, Archivos, Ventas y departamento informático de SUMATEX, con una población de alrededor de 45 personas, siendo la gerente – propietaria la Ing. Susana Guaraca Matute; y, el resto de personal entre empleadas y artesanas (44 personas) distribuidas de la siguiente manera:

Nº	ÁREAS	NUMERO DE PERSONAL
1	Área Administrativa	5
2	Área de Ventas	8
3	Área de Producción	33
4	Área de Almacenamiento	2

Dado al reducido número de personal existente el SUMATEX, para la presente investigación se ha considerado realizar la evaluación y aplicación de cuestionarios a la totalidad del universo, y para la evaluación de los equipos informáticos se toma como muestra la media del universo de 15 equipos.

3.2.1 OBSERVACIONES

SUMATEX cuenta con un número total de equipos informáticos de 15 unidades, de los cuales se tomaron como muestra para el presente estudio, 8 equipos.

3.3 MÉTODOS, TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN

3.3.1 MÉTODOS

Para el presente estudio se utilizaron los siguientes métodos de investigación:

- **Método Deductivo.-** Este método nos permitió deducir de condiciones generales a factores particulares que afectan a SUMATEX.
- **Método Inductivo.-** Con la utilización de este método logramos tener un enfoque global actualizado de la organización y de las alternativas para el cumplimiento de sus objetivos.
- **Método Analítico.-** Este método se lo utilizó con la finalidad de conocer el funcionamiento interno de la organización investigada.
- **Método Sintético.-** Mediante este método analizamos la información existente, lo que nos permitió establecer conclusiones parciales y generales de la investigación.

3.3.2 TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN

Las técnicas que se emplearon en el proceso de investigación fueron la encuesta, la observación, la entrevista y el sondeo.

La encuesta fue aplicada a los empleados involucrados con el manejo de las tecnologías de la información, como son: las jefas de almacenes de ventas, contadora, auxiliar contable, secretaria, jefe del departamento informático y propietaria; lo que se empleó para obtener datos significativos referentes a Operación, Seguridad y Mantenimiento de datos, así como las Seguridades Lógicas, Controles y Seguridades Físicas, para lo que se estructuraron los cuestionarios que fueron un instrumento que permitieron obtener los datos de las áreas de

Informática, Contabilidad, Bodega, Ventas y Producción de SUMATEX. **(Anexo 1: Hojas de cuestionarios de control interno.)**

La observación fue de gran valor en la apreciación de la realidad, circunstancias que permitieron confrontar los hechos e imprimir un sello de transparencia e imparcialidad a la investigación, se utilizó como instrumento el registro de datos para la toma de información de los inventarios de hardware.

Se observó el estado físico del lugar en que se encuentran los equipos informáticos, sus instalaciones, su manejo y protección ante posibles daños. (**Anexo 2: Fuentes de Observación-Tabulación de cuestionarios).**

Las fuentes de observación consideradas para la recopilación de información fueron las áreas donde labora el personal de la empresa, ya que se consideró que los usuarios internos son los que tienen conocimiento claro de lo que es el manejo de los componentes del COSO II, como son: el Ambiente de Interno, el establecimiento de objetivos, la identificación de riesgos, la evaluación de los riesgos, las respuestas a los riesgos, las actividades de control, la información y comunicación y el monitoreo.

Entrevista esta herramienta también se consideró como un aspecto importante en la aplicación y evaluación de la auditoría, ya que gracias a la aplicación de la entrevista preliminar se logró la recopilación de información primordial para evaluar la gestión que se da a la empresa, el manejo al personal, el cumplimiento que se ha dado a los objetivos desde el punto de vista de la dirección.

Sondeo ha sido una herramienta práctica y útil en la aplicación de la auditoría, a través de listas de chequeos y aplicación de indicadores de gestión informática que nos permitieron determinar las medidas de seguridad tanto físicas como lógicas adoptadas en SUMATEX y lo que causa la ausencia de seguridades informáticas para el cumplimiento de objetivos.

AP

SUMATEX

Auditoría de Seguridad Física y Lógica de los Sistemas Informáticos.

Del 01 de Enero al 31 de Diciembre del 2012

ARCHIVO PERMANENTE

Elaborado por:	Inicio	Finalización
SCVC	27/11/2013	06/12/2013

CAPÍTULO IV

4. MARCO PROPOSITIVO: Auditoría de Seguridad Física y Lógica de los Sistemas Informáticos.

4.1 PLANIFICACIÓN DE LA AUDITORÍA

4.1.1. PLANIFICACIÓN PRELIMINAR

En la presente investigación se consideró la información generada durante el año 2012 de la empresa SUMATEX, dedicada a la industria textil; comprendiendo desde el levantamiento de la información hasta la elaboración del programa de auditoría; y a la vez el cumplimiento de tareas como: aplicación de indicadores, evaluación de control interno y asignación del equipo de trabajo.

4.1.1.1 CONOCIMIENTO PRELIMINAR

Este punto tuvo como finalidad realizar un estudio y revisión de la información de la empresa, la recopilación de información automatizada y la visita previa a la entidad para identificar las actividades que se ejecutan en la entidad y determinar la pertinencia y oportunidad de realizar una acción de control.

4.1.1.1.1 RESEÑA HISTÓRICA

SUMATEX inicia sus actividades el 3 de septiembre de 1986, en primera instancia como suministradora de materiales textiles, con la Ing. Susana Guaraca como su Gerente – Propietaria.

En el año 1994 SUMATEX incursiona en la confección de prendas blancas como: sábanas, mantelería, entre otros artículos, con apenas un par de máquinas industriales adquiridas al remate en el Banco Nacional de Fomento.

Posteriormente con el apoyo de créditos comerciales emprende una producción en serie que le permite implementar una planta industrial ubicada en las calles Junín y Palmeras para cubrir una producción de prendas de punto en un 70% y 30% en tejidos planos.

Actualmente la empresa cuenta con una fábrica industrial y tres puntos de venta propios ubicados en: la calle Guayaquil 22- 02 y Espejo; calles Guayaquil entre Colón y Larrea; y, en las calles Junín 25-35 y Palmeras.

4.1.1.1.2 MISIÓN

"La Misión de SUMATEX es confeccionar y comercializar prendas de vestir, de dormir y ropa blanca, que satisfagan necesidades del mercado en forma competitiva, cumpliendo con ética las obligaciones con sus clientes, proveedores, empleados, socios, el Estado y la comunidad en la que se desarrollan las actividades de la empresa"

4.1.1.1.3 VISIÓN

"Ser empresa líder del centro del país en la producción e innovación de prendas de vestir para dormir, así como ser modelo de excelencia en todos sus procesos, reflejada en productos competitivos con fidelidad a sus valores corporativos"

4.1.1.1.4 OBJETIVOS

A largo plazo.- Mejorar la calidad de los productos mediante un estudio de COSTEO ABC y ampliar el mercado de distribución.

A mediano plazo.- Establecer políticas definidas de compra de materiales y venta de productos terminados.

A corto plazo.- Implantar sistemas automatizados de control de inventarios y facturación electrónica en el área de ventas.

4.1.1.1.5 FINALIDAD

- **Producir** prendas de dormir de alta calidad a través de procesos eficientes con tecnología de punta, respeto a la comunidad y al medio ambiente.
- **Buscar** satisfacción del cliente promoviendo innovación, mejoramiento constante y control eficaz de calidad basados en la honestidad y consideración.

- **Motivar** al personal para conseguir ambiente de trabajo agradable y bienestar tanto laboral como personal.

4.1.1.1.6 VALORES CORPORATIVOS

- **Competitividad.-** La competitividad industrial es una medida de la capacidad inmediata y futura del sector industrial para diseñar, producir y vender bienes cuyos atributos logren formar un paquete más atractivo que el de productos similares ofrecidos por los competidores.

- **Confianza.-** Es la seguridad o esperanza firme que alguien tiene de otro individuo o de algo. También se trata de la presunción de uno mismo y del ánimo o vigor para obrar.

- **Lealtad.-** Estamos comprometidos con la Empresa en todo momento, con sus objetivos y metas en forma decidida y constante, obrando siempre con honestidad y justicia.

- **Honestidad.-** Es el valor de decir la verdad, ser decente, recatado, razonable, justo u honrado. Desde un punto de vista filosófico es una cualidad humana que consiste en actuar de acuerdo como se piensa y se siente.

- **Compromiso.-** Engloba a las responsabilidades de todas las personas que componen una sociedad y las capacidades que poseen como grupo.

- R**espeto.-** La persona por encima de todo. Este valor supremo regirá las relaciones entre la organización y sus grupos de interés: clientes, accionistas, trabajadores, proveedores y comunidad.

- **Eficiencia.-** Se refiere a la habilidad de contar con algo o alguien para obtener un resultado**.** Se trata de la capacidad de alcanzar un objetivo fijado con anterioridad en el menor tiempo posible y con el mínimo uso posible de recursos, lo que supone una optimización**.**

4.1.1.1.7 FACTORES INTERNOS Y EXTERNOS

Tabla N° 3: Factores Internos y externos

				
Ambiente Organizacional General				
Condiciones Tecnológicas	**Condiciones Legales**	**Condiciones Económicas**	**Condiciones Políticas**	**Condiciones Sociales**
• Cuenta con equipos informáticos en buenas condiciones. • Maquinaria textil equipada según las últimas tendencias y máquinas que aún están en condiciones favorables.	Basadas en: • El Código Laboral, • Ley de Régimen tributario Interno, • Derecho Tributario, • Régimen de producción artesanal, • Normas de Control Interno, • Cámara de la producción, • Reglamentos y estatutos que regulan el manejo de una industria	Manejadas con un presupuesto financiero estable, superando las fracciones básicas y por tal motivo obligados a llevar contabilidad.	SUMATEX se maneja a la par de los nuevos cambios establecidos por el Estado, cumpliendo a cabalidad las obligaciones tributarias establecidas, y siendo puntual en sus pagos.	• La empresa cuenta con un código de ética y brinda un servicio a la sociedad sin ningún tipo de discriminación social, brindando el mejor servicio acorde al cumplimiento de estándares de calidad, enfrentando de la mejor manera la competitividad; y, trabajando en equipo con liderazgo y

	productora y comercializadora de textiles.			cooperación.
Ambiente Organizacional de Tarea				
Grupos Reguladores	**Competidores**	**Consumidores o usuarios**	**Proveedores**	
• Servicio de Rentas Internas. • Instituto Ecuatoriano de Seguridad Social. • Ministerio de Relaciones Laborales. • Contraloría General del Estado.	• APPAREL FASHION. • MEGASEG. PUNTO CERO. • FABBEC.	• Consumidores Finales. • Entidades del sector público por las que ha sido contratado SUMATEX en el concurso del INCOP. • Gerardo Ortiz • Coral Centro • Coral Rio • Monay • Gerardo Ortiz Guayaquil • Mercantil Tosi	• NILOTEX TELAS S.C.C. • PATPRIMO S.A. • PINTEX S.A. • REINCONEX CIA. LTDA. • SAN PEDRO CIA. LTDA. • MOVE S.A. • MEYTEX • ROLAN S.A. • REINCONEX S.A. • SANTEX • CORTYVIS CIA. LTDA. • FABRINORTE CIA. LTDA.	

Fuente: Datos de la Empresa.
Realizado por: Sandra Valdiviezo.

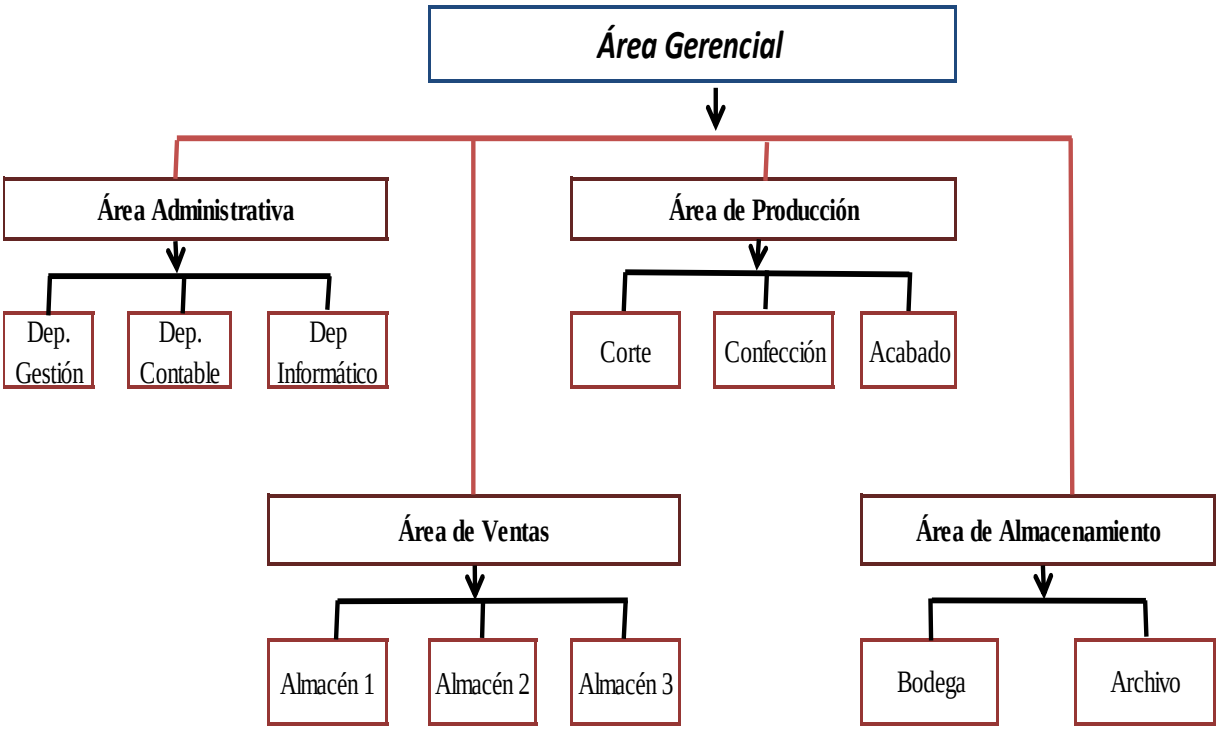
4.1.1.1.8 ESTRUCTURA ORGANIZACIONAL

La estructura organizacional de la fábrica SUMATEX es relativamente sencilla con flujo de información de doble vía (ascendente y descendente), con tres niveles jerárquicos, distribuidos en las siguientes áreas funcionales:

- El Área de Producción con las unidades operativas de corte, confección y de acabado
- El Área Administrativa – Financiera con los Dptos. De Gestión, Contable e Informático
- El Área de Mercadeo y Ventas con sus almacenes 1, 2, y 3
- El Área de Almacenamiento con sus unidades operativas de archivo y bodega

Organigrama Estructural

Ilustración N° 9: Organigrama Estructural



Fuente: Archivo Permanente SUMATEX **Fecha de elaboración:** 14 de Junio del 2008

Realizado por: Consultor Productivo SUMATEX.

Organigrama Funcional

Determina las distintas funciones a cumplirse en la empresa, siendo las siguientes:

Gerente: La administración y gestión de toda la empresa.

Administrador: Responsabilidad realizada por la Gerente.

Jefe de producción: Supervisar y controlar las actividades realizada en la fábrica.

Contador: Llevar la contabilidad de la empresa.

Auxiliar Contable: Realizar registros, actualizaciones y reportes.

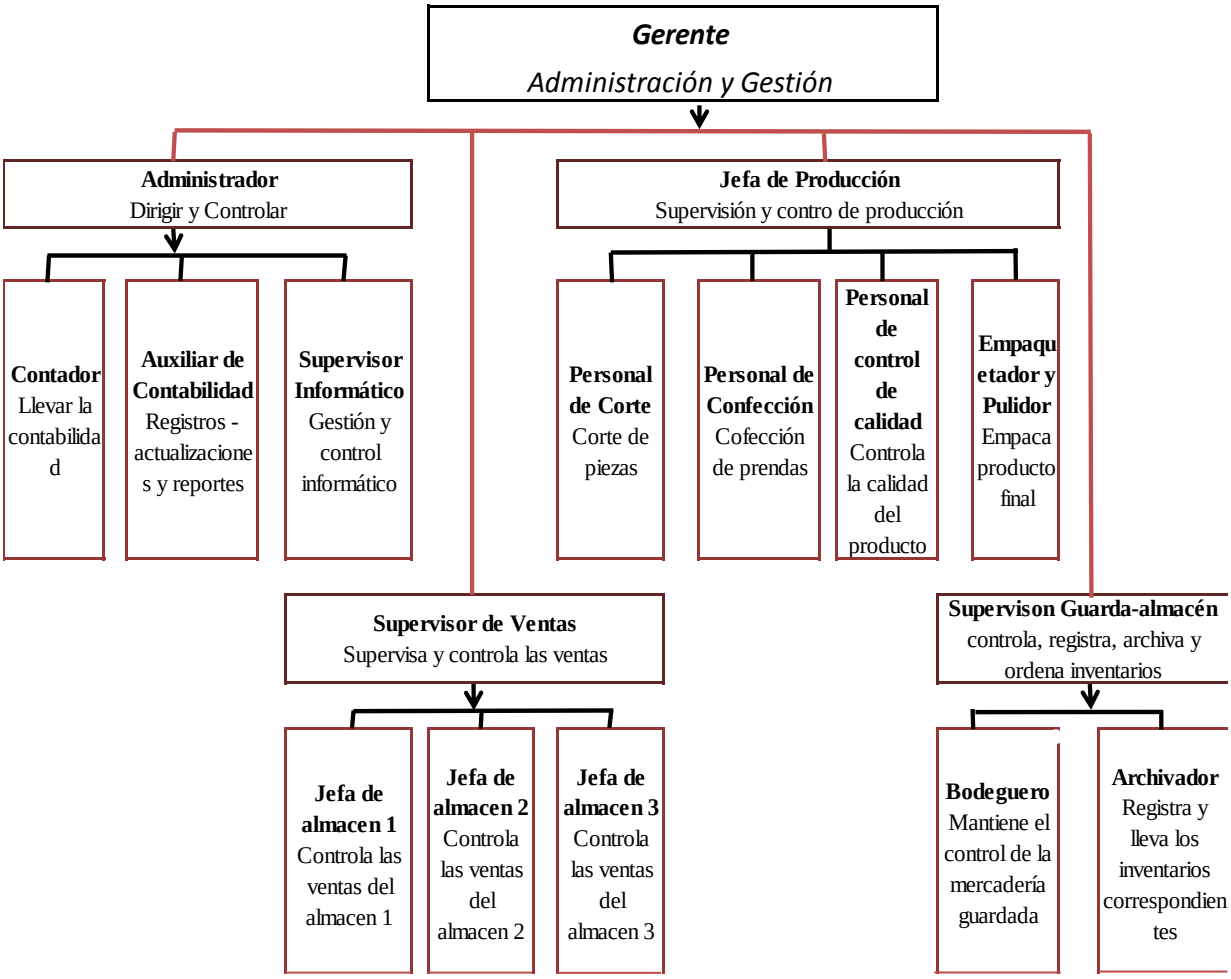
Supervisor Informático: Gestión informática y control.

Personal de producción: Encargada de la producción de prendas y cumplimiento de lo encomendado.

Supervisores de Ventas: Supervisar y controlar el normal desarrollo de los locales de distribución directa en ventas.

Supervisor Guarda - almacén: Controlar, registrar, archivar, ordenar y embodegar la mercadería terminada existente en la empresa.

Ilustración N° 10: Organigrama Funcional

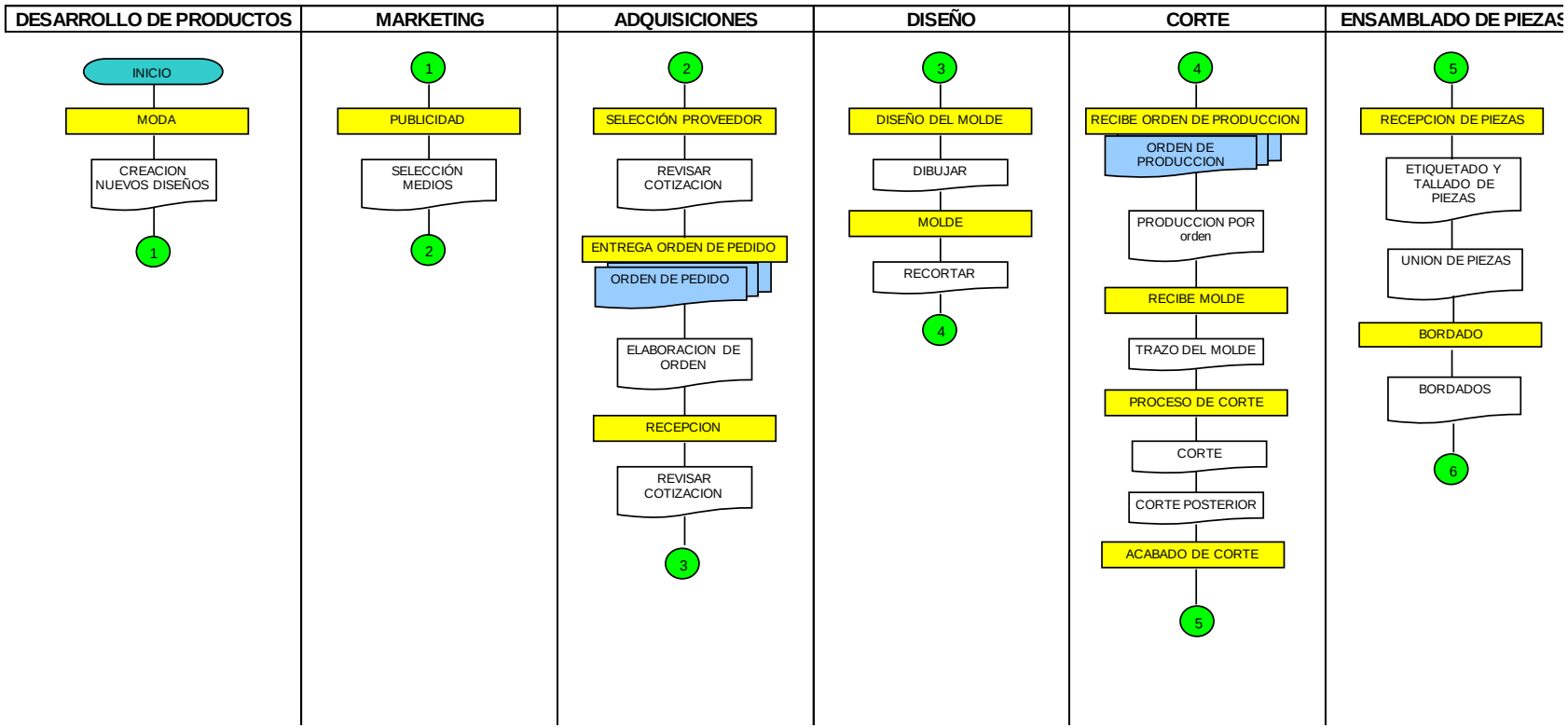


Fuente: Archivo Permanente SUMATEX **Fecha de Elaboración:** 14 de Junio del 2008.

Realizado por: Consultor Productivo SUMATEX.

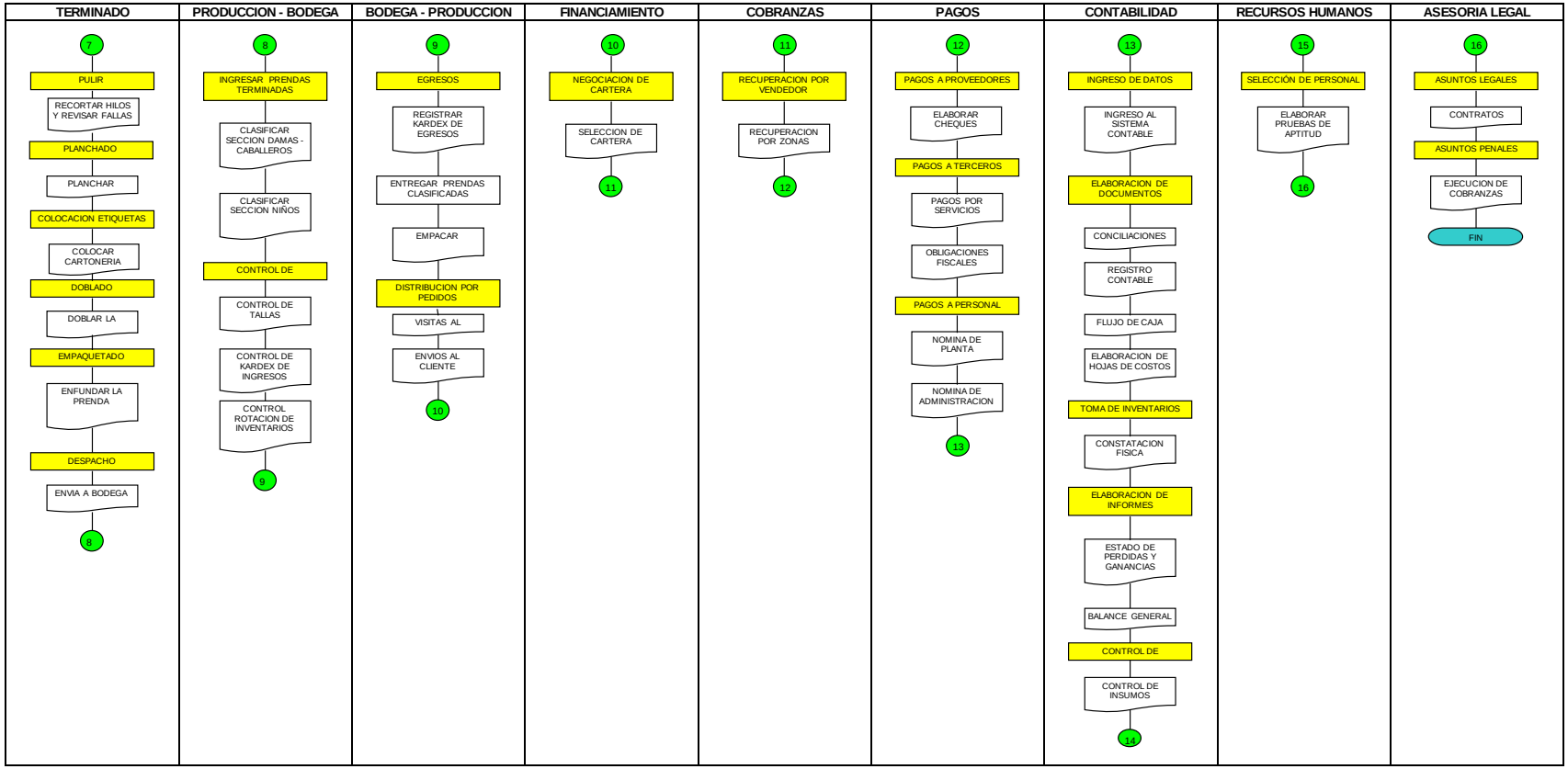
4.1.1.1.9 FLUJOGRAMA DE PROCESOS – ACTIVIDADES – TAREAS

Ilustración N° 11: Flujo grama de procesos.

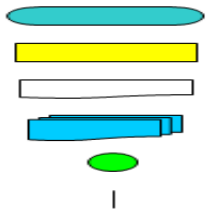


Fuente: Archivo Permanente SUMATEX

Realizado por: Consultor Productivo SUMATEX.



SIMBOLOGIA:



INICIO O FIN

ACTIVIDAD DEL PROCESO

TAREA DE LA ACTIVIDAD

DOCUMENTO

CONECTOR

DIRECCIONAMIENTO

Fuente: Archivo Permanente SUMATEX

Realizado por: Consultor Productivo SUMATEX

4.1.1.1.10 FUENTES DE FINANCIAMIENTO

SUMATEX inició con un capital propio de S/.300.000,00 Sucres y en el transcurso del tiempo fue creciendo con créditos bancarios adquiridos en el Banco del Pichincha, los que han sido cancelados de manera parcial y puntual con lo acordado, hasta lograr un capital actual de $349.668.04

4.1.1.1.11 FUNCIONARIOS PRINCIPALES

Tabla N° 4: Funcionarios Principales

CARGO	NOMBRE DEL FUNCIONARIO
Gerente General:	Ing. Elsa Susana Guaraca Matute
Contadora:	Ing. Paulina Ayala
Consultor Productivo:	Ing. Andrés Posada Hernández.
Supervisor Informático:	Ing. Pablo Cruz.
Jefe de Producción:	Srta. Nancy Saca.
Jefe de Bodegas:	Srta. María Pilco.
Supervisor de Ventas:	Sra. Margarita Muñoz

Fuente: Datos de la Empresa.

Realizado por: Sandra Valdiviezo.

4.1.1.2. INFORME DE CONOCIMIENTO PRELIMINAR

4.1.1.2.1 DATOS GENERALES

Logo:

Nombre Empresa: SUMATEX

Representante Legal: Ing. Susana Guaraca

RUC: 1500317605001

Tipo De Contribuyente: Obligado a llevar contabilidad

Planta Industrial: Junín 45-37 y Las Palmeras

Teléfono: (03)2960192

Calificación Artesanal: Junta de Defensa del Artesano Nº 82908

Rama Artesanal: Corte y confección.

Correo: sumatexsg@hotmail.com

Actividades:

- **Actividad Económica Principal**

  Fabricación de prendas de vestir para dormir de damas, caballeros y niños.

- **Actividades Económicas Secundarias**

  Fabricación de ropa blanca, edredones, sábanas, ropa de baño, etc.

4.1.1.2.2 DATOS EMPRESARIALES

Matriz: Riobamba - Guayaquil 22-02 y Espejo

Sucursales: Riobamba - España 20-39 y Guayaquil

Riobamba - 10 de Agosto s/n y Rocafuerte

Distribuidora: Riobamba - Junín y Palmeras.

Nº de empleados: Producción: 27 empleados

Personal Administrativo: 7 personas

Personal de Ventas: 8 personas

Personal bodegas: 3 personas

Maquinaria Existente: 26 máquinas de operación y 6 complementarias.

Capacidad de Producción: 12.200 prendas mensuales en temporada normal; y hasta 25.100 prendas en temporada alta.

Destino de Producción

Tabla N° 5: Destino de la Producción

COSTA	SIERRA	ORIENTE
Esmeraldas	Quito	Tena
Portoviejo	Tumbaco	Lago Agrio

Calceta	Santo Domingo	
Manta	Latacunga	
Chone	Salcedo	
Guayaquil	Ambato	
Machala	Guaranda	
Quevedo	Riobamba	
Tosagua	Cuenca	
	Loja	

Fuente: Datos de la Empresa.

4.1.1.2.3 INDICADORES DE GESTIÓN

I.G. 1/3

Tabla N° 6: Indicadores de Gestión Informática

ACTIVIDAD	ASUNTO	FÓRMULA
Costo	Costo de informática en relación al costo administrativo.	Costo Total de informática / Costo total de administración
	Costo de informática en relación a los ingresos de la empresa.	Costo Total de informática / Ingresos totales de la empresa
	Costo de informática por empleado.	Costo Total de Informática / Número Total de empleados
	Costo medio por ordenador (PC)	Costo total de compra y mantenimiento de los PC / Número de los PC
	Costo de mantenimiento	Costo de mantenimiento informático / Costo total informático

Incidencias	Incidencias debidas al no respeto de la política informática en relación a las incidencias	Número de incidencias debidas al no respeto de la política informática / número total de incidencias
	Tiempo medio con sistema no disponible	Tiempo con sistema no disponible / tiempo total operativo
	Tiempo medio entre fallas	(tiempo operativo – tiempo no disponible) / número de fallas
Infraestructura	Tiempo medio del cambio de los equipos	Tiempo medio entre la identificación de la necesidad de cambio y el cambio efectivo
	Número medio de ordenadores PC por empleados	Número de PC / Número de empleados
	Número medio de impresoras por departamento	Número de impresoras / Número de departamentos
RRHH	Tiempo dedicado a actividades informáticas innovadoras	Tiempo dedicado a actividades innovadoras / Tiempo de trabajo total en informática
	Formación	Número de horas de formación / número de empleados en informática
	Nómina de sueldos	Nómina de sueldos informática / Total Nómina de sueldos
	Estabilidad	Número de empleados presentados después de 6 meses / Número de nuevos empleados contratados hace 15 meses
		Edad media de los empleados
Seguridad	Seguridad Lógica	Nº de incidencias/solicitudes

		atendidas en un mes
		Número de incidencias atendidas / número de incidencias recibidas.
	Seguridad Física	Riesgos identificados / posibles riesgos
		Número de medidas de seguridad tomadas / posibles medidas de seguridad existentes
		Número de accesos de personal desautorizados / Número de control de acceso a los equipos informáticos

Fuente: Datos de la Empresa.

Realizado por: Sandra Valdiviezo.

4.1.1.2.4 ANÁLISIS SITUACIONAL DE LA EMPRESA SUMATEX

A.S. 1/5

ASPECTOS IMPLICADOS

- Gran número de empresas de la competencia en el mercado, en cuanto a la línea de producción a la que se dedica SUMATEX.
- Inadecuado sistema de incentivos al personal, a través de comisiones, horas extras, alimentación, entre otros.
- Posible cierre de acuerdos contractuales con Mi Comisariato y otras cadenas de ropa, lo cual incrementaría considerablemente las ventas y exigiría mucho más de la producción.
- Falencias en imagen corporativa y posicionamiento gráfico en el mercado.
- No hay concordancia entre la demanda, la cantidad que se produce y la comercialización; en el caso de la fábrica SUMATEX la demanda es mucho mayor a la comercialización y producción.

- No hay uso de indicadores que sirvan para renovar la materia prima y eso origina complicaciones de producción.
- Experiencia en el mercado y en la producción.
- Dominio del corte y confección por parte de la mano de obra.
- No existen políticas de renovación de colecciones de ropa.
- Indisciplina en el personal respecto la hora de entrada, permisos y hora de salida.
- No existe privacidad de información acorde a las funciones, por lo cual cualquier persona que tenga acceso a las computadoras puede modificar la información con o sin intención.
- Pericia por parte de la Jefa de Producción quien dirige de forma excelente su área de trabajo y supervisión.
- Falta de reuniones y conferencias para fomento de relaciones humanas e integración.
- Constante capacitación del personal de producción que cubre totalmente la empresa.
- No se cuenta con el personal de comercialización propio, sino únicamente como comisionistas.
- Falta de publicidad sobre la empresa, identidad, marca y productos que se elaboran.
- Inmuebles hipotecados sin créditos prendarios.

ASPECTOS ECONÓMICOS

- Bajas remuneraciones acorde las funciones y desempeño de los trabajadores.
- Manejo empírico del financiamiento de la empresa;
- Adecuado costeo de inventario.
- Alto porcentaje de morosidad en cartera al por mayor.
- Mal manejo de cartera vencida.
- Adecuadas políticas de precios, resultando éstos competitivos en el mercado y con un considerable porcentaje de utilidad.
- Inadecuado manejo de políticas financieras y costeo de gastos por concepto de intereses y financiamiento en general.
- No existe elaboración, ni ejecución presupuestaria.

- Falta de un adecuado control de inventarios.
- Independencia del punto de distribución en Guayaquil, sin embargo hay falencias en cuanto al control de facturación y pago.
- Récord impecable en el Buró de Crédito, lo cual es una gran ventaja para el otorgamiento de créditos nuevos.
- Flujo lento de información de cobros y pagos.

ASPECTOS POLÍTICOS

- Con el tema de restricción de ciertos productos de importación o el bajo cupo de los mismos para el mercado, se ha reducido la disponibilidad de materia prima y se han suprimido varios tipos de productos.
- Política gubernamental de fomento a la producción interna a través de incentivos en capacitación y otorgamiento de créditos.
- Falta de apoyo de los gobiernos seccional y local a la producción riobambeña sin brindar incentivos, beneficios u otros.

ASPECTOS SOCIO – CULTURALES

- Poco conocimiento de los riobambeños de la empresa y el reconocimiento que tiene a nivel nacional.
- No existen políticas de vinculación con la comunidad.

ASPECTOS AMBIENTALES

- Caso omiso de normas de seguridad industrial, tanto por parte de la administración, como del personal en general.
- Optimización de materia prima evitando desperdicios innecesarios, esto se debe gracias a un sistema de reciclaje y venta de retazos.

ASPECTOS JURÍDICOS

- Beneficios arancelarios fruto de pertenecer a la rama y régimen artesanal.

- Falta de contratos escritos de trabajo, el 90% de contratos son tácitos; esto puede generar problemas con los empleados, así como con los entes de control (Ministerio de Relaciones Laborales y el IESS).
- Empresa constituida como persona natural.

ASPECTOS ADMINISTRATIVOS – ORGANIZACIONALES

- Deficiencia en los canales de comunicación, ya que la información no es canalizada formalmente a través de documentos, sino de forma verbal, lo cual origina confusión y falta de evidencia para futuras auditorías.
- Manejo al azar y sin sustento técnico de las relaciones y estrategias comerciales, lo cual impide la expansión de la empresa.
- Falta de una adecuada estructura organizacional que permita delimitar funciones y responsabilidades a los trabajadores.
- Falencias en la toma de decisiones parte de los directivos de la empresa, ya que no se consideran los datos o información real, sino las expectativas o pensamientos de su gerente.
- Adecuada organización de la producción en línea, acorde a las demanda por temporadas.
- Falta de implementación de una agenda de comercialización.
- Adecuado manejo de las relaciones humanas por parte de la gerencia, lo cual genera lealtad, respeto, consideración y otros valores corporativos.
- Fallas en la delegación de autoridad y responsabilidad, particularmente en el área de producción, ya que en el proceso de requisición de materia prima se solicita autorización a la administración, cuando lo pertinente debería ser el jefe productivo quien tenga la potestad para hacerlo; esto desacelera dicho proceso y ocasiona incurrimiento en costos.

ASPECTOS TECNOLÓGICOS

- Se cuenta con tecnología moderna para la producción de prendas y su control de calidad.

A.S. 5/5

- Deficiente sistema informático de control interno.
- Falta de implementos tecnológicos que permitan desarrollar mejores técnicas de patronaje.

ASPECTOS ESTRUCTURALES

- Inadecuada estructura de la planta industrial, ya que no permite ampliar su producción por falta de espacio.
- Falta de espacio para almacenamiento de la producción.
- Deficiente estructura organizacional al concentrar funciones en determinadas personas, lo cual produce conflictos por evasión, arrogación y duplicación de actividades.

SITUACIÓN ACTUAL DE LA FÁBRICA

Al momento, los productos que se elaboran en la empresa SUMATEX, se manipulan bajo un registro de entrada y salidas de tipo manual, el cual no es fiable en un 100%; es por ello que se hace necesario instalar un software de facturación e inventarios acordes a las necesidades y requerimientos particulares de la empresa, al tiempo de delegar a una persona para que sea la responsable de mantener la información actualizada.

OBJETIVOS

Conocer el valor del inventario, cualitativa y cuantitativamente, a fin de poder tomar acciones correctivas en el momento oportuno.

SOLUCION DEL PROBLEMA

Esta área recaerá sobre una persona "X" la cual se encargará de manipular un sistema que nos permita controlar la bodega en lo referente al área de inventarios, tanto numérica como físicamente, y así emitir informes al departamento que está subordinado.

Para que los objetivos de esta área se cristalicen es necesario que se implante un sistema apropiado de facturación e inventarios, el cual le permitirá emitir los reportes eficaz y oportunamente.

A.F. 1/3

4.1.1.2 ANÁLISIS FODA

Detección de las Fortalezas, Debilidades, Oportunidades y Amenazas.

Tabla N° 7: Análisis FODA

Fortalezas	**Oportunidades**
1. SUMATEX tiene un sistema de distribución rápida y segura. 2. Su fábrica y oficinas administrativas están ubicadas en instalaciones propias lo que le ayuda a la disminución de gastos. 3. Posee maquinaria con tecnología de punta. 4. Los equipos informáticos se encuentran en buenas condiciones y siempre a disposición. 5. Posee su propio sistema informático administrativo. 6. Sistema de reciclaje y optimización de materia prima.	1. Cumple con los requerimientos y condiciones que requiere el sector público para participar en sus concursos del INCOP. 2. Posee buenas relaciones y contactos con empresas importantes. 3. Incursión a nuevos mercados internacionales con productos de buena calidad. 4. Posibilidades de concursar en ferias internacionales para promocionar los productos. 5. Capacitaciones constantes del SRI, y técnicos en informática que realizaron su programa administrativo. 6. Récord impecable en el Buró de Crédito. 7. Política gubernamental de fomento a la producción. 8. Privilegios arancelarios acorde al régimen artesanal.

A.F. 2/3

DEBILIDADES	AMENAZAS
1. No posee la infraestructura necesaria para ampliar su fábrica. 2. No posee seguridades físicas y lógicas óptimas. 3. Desconocimiento del personal de las políticas informáticas, las normas internas de la empresa y los objetivos a alcanzar. 4. No se han realizado análisis de los riesgos a los que se enfrentan los equipos informáticos, tanto físicos como lógicos. 5. Desconocimiento de las seguridades que se pueden adoptar para aplicar en la empresa. 6. No posee soportes de información en un lugar distinto a la empresa. 7. Falta de imagen corporativa. 8. Incómodo ambiente de trabajo en el área productiva. 9. Falta de producción para cubrir demanda. 10. Falta de indicadores para renovar la materia prima.	1. La existencia de una gran cantidad de virus informáticos que pueden afectar los sistemas automatizados de la empresa. 2. Empresas modernas de la competencia, altamente eficientes, y grandes en: producción, sistematización y/o automatizadas. 3. Las grandes amenazas en el mundo del internet por la presencia de hackers y crackers. 4. Poca seguridad física que salvaguarde los recursos. 5. Falta de tecnología informática, que reduzca los costos operativos. 6. Ingreso de productos importados con calidad certificada y a menor costo. 7. Restricción de importación de materia prima. 8. Poco apoyo de los gobiernos: seccional y local. 9. Exceso de competencia en el mercado.

A.F. 3/3

11. Falta de publicidad. 12. Bajas remuneraciones al personal. 13. Empirismo en el manejo del financiamiento. 14. Inadecuado control de inventarios. 15. Inadecuado sistema de cobros y pagos. 16. Falta de políticas de vinculación con la comunidad. 17. Omisión en normas de seguridad industrial. 18. Inestabilidad laboral ante la constante firma de contratos de trabajos tácitos. 19. Deficiencia en los canales de comunicación. 20. Empirismo en las relaciones y estrategias comerciales. 21. Inadecuada estructura organizacional. 22. Falencias en la toma de decisiones. 23. Inadecuada delimitación de funciones y responsabilidades. 24. Deficiente sistema informático de control interno. 25. Falta de tecnología para patronaje. 26. Sistema informático de contabilidad desactualizado. 27. Inadecuada Bodega de almacenaje.	

Fuente: Datos de la Empresa.
Realizado por: Sandra Valdiviezo.

ECI. 1/1

4.1.1.3 ESTRUCTURA DE CONTROL INTERNO

SUMATEX no tiene estructurado de manera formal un sistema de control interno, pero si se han tomado medidas para este fin, que han ayudado al normal desenvolvimiento de las actividades, entre estas: disponibilidad de manuales de procesos, flujo gramas de procesos, instructivos de actividades - tareas y políticas internas.

4.1.1.4 DEFINICIÓN DEL OBJETIVO Y ESTRATEGIA DE AUDITORÍA

4.1.1.4.1 Objetivo de la Auditoría

La Auditoría de la seguridad física y lógica de sistemas informáticos tiene como objetivo evaluar el grado de protección del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los albergan. El auditor informático debe contemplar situaciones de incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc., que pueden afectar la protección de los recursos informáticos de SUMATEX, o impedir el cumplimiento de los objetivos organizacionales.

4.1.1.4.2 Auditoría de Seguridad Física y Lógica

Para la realización de la auditoría de Seguridad Física y Lógica, se realizó el estudio previo de la información contenida en los archivos propios de la empresa SUMATEX, el que se incluyó dentro de la Planificación preliminar, a la vez, se determinó las áreas críticas, se evaluaron los riesgos, se aplicaron los papeles de trabajo y se emitió el correspondiente informe de auditoría como un aporte para la mejor toma de decisiones.

4.1.1.5 DESIGNACIÓN DEL EQUIPO DE TRABAJO

Para la ejecución de la Auditoría fue de suma importancia el apoyo de los administradores de SUMATEX, ya que con su apertura se logró la recopilación de la información suficiente y competente para el cumplimiento del programa de auditoría; al igual que se necesitó la ayuda

del Supervisor informático como poseedor del conocimiento necesario sobre el manejo de los sistemas, el control que se lleva y el funcionamiento del sistema en general.

Fue asimismo necesario el apoyo incondicional del personal operativo de la empresa para la determinación de hallazgos y el éxito del presente examen de auditoría.

4.1.1.6 TIEMPO UTILIZADO

El presente examen de auditoría de Seguridad Física y Lógica de Sistemas Informáticos se estimó hacerlo en un tiempo estimado de 90 días laborables, periodo considerado suficiente para analizar y evaluar los distintos procesos que se ejecutan en la Empresa SUMATEX.

4.1.2 PLANIFICACIÓN ESPECÍFICA

4.1.2.1 RECOPILACIÓN Y ANÁLISIS DE INFORMACIÓN

En esta fase se recopiló y analizó la información relacionada a la organización, sus operaciones y el control interno; a partir de aquello se determinó las áreas críticas, el alcance de la auditoría, los programas y finalmente el memorando de planificación.

4.1.2.2 MANUALES E INSTRUCTIVOS VIGENTES

4.1.2.2.1. Manual de Funciones (Detalle de Funciones y Responsabilidades)

1. **Gerente General**

El gerente general, será el encargado de administrar el ente económico con buen juicio, criterio, honestidad y responsabilidad. Dentro de sus funciones comprenden:

- Velar por el buen funcionamiento de los departamentos de la empresa,
- Negociar fuentes de financiamiento,
- Desarrollar negociaciones comerciales en pro de incursionar en nuevos mercados,
- Abastecer de materiales a la producción,
- Ser representante legal de la empresa,
- Asumir responsabilidades patronales, etc.

2. Jefe de Producción

El jefe de producción será un profesional del área de corte y confección cuyas funciones comprenden:

- Vigilar los procesos de producción en todas sus áreas,
- Solicitar a la gerencia cuando sea necesario los materiales para el desarrollo de las actividades del departamento;
- Controlar asistencia, puntualidad y orden en el grupo obrero;
- Organizar los grupos de trabajo;
- Tomar las pruebas de ingreso a los aspirantes a obreros;
- Diseñar patrones y moldes;
- Establecer nuevos productos y líneas de producción; etc.

3. Jefe Financiero – Contadora

El jefe financiero o contador será un profesional del área financiera encargado de desarrollar las siguientes actividades:

- Llevar ordenada y prolijamente al contabilidad de la empresa,
- Establecer precios,
- Determinar costos de producción,
- Realizar roles de pago a todo el personal,
- Analizar las fuentes de financiamiento convenidas,
- Declarar impuestos,
- Organizar los planes estratégicos y presupuestos,
- Llevar sistemas de control interno, etc.

4. Vendedores

Los vendedores tendrán como funciones:

- Analizar el mercado y ofrecer las líneas de productos;
- Hacer pedidos a producción,
- Receptar mercadería o en su defecto facturas al cobro;
- Cobrar a los clientes; etc.

4.1.2.2.2 Instructivos

a) Área de Control de Calidad y Empacado

Esta responsabilidad recaerá sobre las personas que se encargan de cortar hilos, etiquetar y enfundar; es necesario que en el transcurso de este proceso se verifique si existen fallas, en caso de que las hubiese, se reintegren las prendas al personal que las entregó para que procedan a corregir.

También es importante que consideren la seriedad del trabajo que desarrollan, ya que si pasan por alto algún error o a su vez lo cometen (Mal Codificado – Falta de algún elemento de la Prenda si constituye conjunto), la responsabilidad recaerá sobre las personas que integran esta área

b) El Área de Diseño y Área de Cortado

Las responsabilidades del Cortado recaerán sobre la Srta. Lorena Narváez, conjuntamente con su auxiliar la Srta. Blanca Ocaña, quienes se encargarán de entregar a los departamentos de ensamblado las piezas necesarias para la confección de las prendas; en este proceso se hace necesario la coordinación con el responsable del área de bodega, quien se encargará de surtir los elementos que complementan las prendas a confeccionar (hilos, etiquetas, tallas, botones, encaje, etc.).

c) El Área de Ensamblado

Esta responsabilidad recaerá sobre las personas que unen las prendas, mismas que tienen que entregar los artículos terminados a la siguiente área que les sucede (El Área de Control de Calidad y Empacado). Las prendas a entregar será en el mismo número que a ellos les fue entregado, en caso de daño o pérdida de alguna de ellas será responsable la persona a la que le fue destinada esta tarea.

d) El Departamento de Contabilidad

Esta responsabilidad recae sobre el Contador, quien se encarga de emitir informes de situación financiera de la empresa a la Gerencia, siendo sus principales funciones las siguientes:

- Llevar un sistema único de contabilidad.
- Presentar e interpretar los resultados de los estados financieros.

- Declarar los impuestos de la empresa en las fechas establecidas y de acuerdo a la Ley de Régimen Tributario Interno.
- Organizar la contabilidad.
- Desarrollo de la nómina de los trabajadores.
- Elaboración de hojas de costos, entre otras.

e) Área de Costos

- Mantener una coordinación con la gerencia, para la adquisición de la nueva maquinaria y materia prima a utilizarse en los diferentes procesos.

f) El Departamento de Producción

Situación Actual

Al momento los procesos que se desarrollan en la empresa son meramente empíricos, procesos que si se equiparan con la técnica su desarrollo será más eficiente, y por lo tanto generará un desarrollo sustentado en la Fábrica.

Objetivos

- Optimizar los recursos que la empresa dispone al momento, con la finalidad de mejorar el nivel de producción y por ende el nivel de ventas a través de herramientas de gestión.
- Dotar de las herramientas necesarias.
- Distribuir uniformemente las tareas.
- Comunicar.
- Incentivar.
- Planificar y Presupuestar numéricamente los productos a elaborar, para lo cual se trabajará conjuntamente con el área de inventarios, puesto que éste es quien proveerá de todos los elementos con que se elaborará las prendas.

g) El Departamento de Ventas

Este departamento lo integran tres agentes que se encuentran subdivididos en las siguientes zonas:

- Zona Sierra Norte – Centro.
- Zona de la Costa.
- Zona Oriental.

En tanto, que en la ciudad de Riobamba existen Supervisores de Ventas para cada almacén responsables de optimizar la distribución de los productos.

Tabla Nº 8: Distribución de tareas.

PROCESOS	ACTIVIDADES	TAREAS	RESPONSABLE
1. Desarrollo de productos.	Moda.	Creación de nuevos diseños.	Ing. Susana de Robalino Srta. Lorena Narváez
2. Marketing.	Publicidad.	Selección de medios de comunicación.	Ing. Susana de Robalino
3. Adquisiciones.	Selección de proveedor.	Revisar cotización.	Ing. Susana de Robalino
	Entrega orden de pedido.	Elaboración de orden.	Srta. Lorena Narváez
	Recepción.	Constatación física.	Srta. María F. Salazar
4. Diseño.	Diseño del molde.	Dibujar.	Srta. Lorena Narváez
		Recortar.	Srta. Lorena Narváez
	Orden de producción.	Definir escala.	Srta. Lorena Narváez
		Definir volumen de producción.	Ing. Susana de Robalino
5. Corte.	Recibe orden de producción.	Producción por lote.	Srta. Lorena Narváez
	Recibe molde.	Trazo del molde.	Srta. Lorena Narváez
	Proceso de corte.	Corte delantero y posterior	Srta. Blanca Ocaña
		Corte de piezas restantes.	Srta. Blanca Ocaña

6. Ensamblado de Piezas.	Recepción de Piezas.	Etiquetado y tallado de piezas.	Arévalo Silvia, Arévalo Gloria, Arévalo María, Chávez Carmen, Cordovéz Viviana, Manzano Elena, Manzano Ximena, Narváez Lorena, Ocaña María, Saca Nancy, Tiuma Ana, Yance Paulina, Bonilla Lourdes, Jaramillo Margarita.
		Unión de piezas.	Lucrecia Tenemasa, Silvia Cuichan, Uvidia María.
		Bordado.	Rolantex
7. Tercerización.	Hacer ojales.		Arévalo Silvia
			Arévalo Gloria
			Arévalo María
			Chávez Carmen
	Pegar botones.		Cordovéz Viviana
			Manzano Elena
			Manzano Ximena
			Narváez Lorena
	Hacer ribetes.		Ocaña María Piedad
			Saca Nancy
			Tiumi Ana
			Yance Paulina
			Bonilla Lourdes
	Pegado de pretinas.		Jaramillo Margarita
			Lucrecia Tenemasa
			Silvia Cuichan
	Elaboración de bastas.		Uvidia María

8. Terminado	Pulir.	Recortar hilos.	Ocaña Carmen
		Revisar fallas.	Saca Ximena
		Planchar.	Barahona Esthela
		Colocar cartonería y códigos.	Ocaña Carmen
		Doblar la prenda.	Saca Ximena
		Enfundar la prenda y embodegar	Barahona Esthela
9.Producción a Bodega	Recibe prendas terminadas.	Clasificar sección damas.	Responsable de Bodega
		Clasificar sección caballeros.	
		Clasificar sección niños.	
	Control de inventarios.	Control de tallas.	
		Control de kárdex.	
		Control rotación de inventarios.	
10.Bodega a Producción	Control de egresos	Registrar kárdex de ventas o egreso.	
		Entregar prendas confeccionadas.	
		Empacar.	
11. Financiamiento	Negociación de cartera	Selección de cartera.	Ing. Susana de Robalino
12. Cobranzas	Recuperación por vendedor	Recuperación por zonas.	Sr. Eduardo Trujillo
			Sr. Carlos Ibarra
13. Pagos	Pagos proveedores	Elaborar cheques.	Ing. Susana de Robalino
	Pagos a terceros	Pagos por servicios.	Srta. María F. Salazar
		Obligaciones fiscales.	Sr. Marco Ruiz

	Pago a personal	Nómina de planta.	Ing. Susana de Robalino
		Nómina de administrativo	Ing. Susana de Robalino
14. Contabilidad	Ingreso de datos	Ingreso al sistema contable.	Paulina Ayala
	Elaboración de documentos	Conciliaciones.	Srta. Jenny López
		Registro contables.	Marco Ruiz
		Flujo de Caja.	Srta. María F. Salazar
		Elaborar Hojas de costos.	Marco Ruiz
	Toma de inventarios	Constatación física.	Marco Ruiz y Auxiliar de Bodega.
	Elaboración de Informes	Estado de Pérdidas y Ganancias.	Paulina Ayala
		Balance General.	Paulina Ayala
	Control de inventarios	Control de Insumos.	Auxiliar de Bodega
15. Recursos Humanos	Selección de personal	Elaborar pruebas aptitud.	Ing. Susana de Robalino Srta. Lorena Narváez
16. Asesoría legal	Asuntos Legales.	Contratos.	Opcional
	Asuntos Penales.	Ejecución de cobranzas.	Opcional
17. Informático	Control e innovación de la Tecnología.	Control del manejo de los equipos Informáticos. Manejo de los sistemas administrativos y contables.	Ing. Pablo Cruz

Fuente: Datos de la Empresa.

Realizado por: Asesor Productivo.

4.1.2.2.3 Manual del Usuario del Sistema Administrativo

a) Multifinalitario "Saraí"- "SSiAM".

SSiAM© - Saraí, Sistema Administrativo Multifinalitario

SSiAM es un Sistema que permite realizar de una manera ágil y sencilla las tareas más importantes de una empresa o negocio, sobre las cuales desea mantener un mejor control en el flujo de la Información, esto es: Inventarios, Facturaciones, Cuentas por Cobrar, Cuentas por Pagar, Bancos y Contabilidad. Es un Software de fácil uso, pues si ha realizado una factura a lápiz y papel, entonces con SSiAM puede hacerlo; no necesita ser especialista en computación ni tener altos conocimientos contables para obtener los resultados deseados.

Todos los Módulos del Sistema son de similares características, pensando siempre en los usuarios y en la pronta concepción del mismo. Saraí, Sistema Administrativo Multifinalitario "SSiAM" (mono o multiusuario) está conformado por los siguientes Módulos:

1. Inventarios
2. Facturaciones
3. Cuentas por Cobrar
4. Cuentas por Pagar
5. Bancos
6. Contabilidad Anual del Usuario

b) Conceptos Generales del Sistema

Son las diferentes características o conceptos que se aplican a nivel general en todos los Módulos y Opciones del Sistema:

- Cómo ingresar a un módulo o sub-módulo y/o cómo elegir una opción.
- Cómo seleccionar un determinado artículo o cuenta.
- Que es un campo.
- Tipos de Documentos, etc.

c) Módulos del Sistema:

1. Inventarios

Como su nombre lo indica, controla el flujo de los artículos, productos o servicios que brinden o existan dentro de su Inventario (permite llevar el control hasta de 4 Bodegas), asignando códigos a cada uno de ellos, consultando en cualquier momento los precios de venta, costos, kárdex, etc.

Inventarios, está conformado por los siguientes sub-módulos:

- Artículos
- Movimientos
- Procesos
- Reportes
- Utilitarios
- Salir

En general, el Manual del Sistema SSiAM, es un documento que describe de manera específica el manejo adecuado del sistema, las funciones que posee y las finalidades de cada uno de ellos con relación al cumplimiento de las necesidades de SUMATEX.

4.1.2.3 FUNCIONARIOS PRINCIPALES

NOMBRES Y APELLIDOS	CARGO	PERMANENCIA EN EL CARG
ELSA SUSANA GUARACA	GERENTE GENERAL	22 AÑOS

La Gerente es Ingeniera en Administración de Empresas y tiene conocimientos en tiempos y movimientos.

- Jefa de Producción: Nancy Saca.
- Contadora: Paulina Ayala.
- Asistente de contabilidad: Jenny López.
- Supervisor Informático: Ing. Pablo Cruz.
- Asesor de Producción: Ing. Andrés Posada Hernández.

Número de Empleados de la Entidad

Nº de Empleados: Producción: 30 empleados, personal administrativo: 7, personal de Ventas: 8 personas

4.1.2.4. POLÍTICAS COMERCIALES

a) Stock.- La empresa maneja una política en cuanto al stock de existencias, es decir, se deberá contar siempre con un pequeño número de unidades en el inventario final, con el objeto de en caso de imprevistos o de desabastecimiento se pueda responder frente a los clientes al por menor.

b) Comercialización.- En cuanto a la política de comercialización se vende al por mayor en una relación 60/40, es decir 60% al contado y 40% a crédito; y, al por menor en una relación 90/10, es decir 90% al contado y 10% a crédito; esto se debe a que al por mayor se trata de ser consecuente con el cliente quien espera de sus ventas obtener los fondos para el pago. En cambio, en el caso de las ventas al por menor solo es el 10% a crédito, ya que se considera los convenios institucionales que mantiene la empresa con sus clientes de varias entidades y organismos del sector público y privado.

También se debe mencionar en cuanto a la política de comercialización que se planifica dando prioridad a la producción, al por mayor con un 70% vs. un 30% al por menor.

c) Precios.- Para la política de precios la empresa considera un margen de utilidad aproximado del 65% sobre el costo para la venta al por menor; y, para la venta al por mayor un 15%.

d) Costos.- En la política de costos se debe resaltar que al considerar los Costos Indirectos de Fabricación se han establecido estándares fijos.

e) Sueldos.- La política de sueldos está sujeta a lo que determina el Ministerio de Relaciones Laborales en cuanto al régimen de producción artesanal, que señala los sueldos para artesanos y actividades de confección de prendas de vestir y otras, siendo los siguientes:

Tabla N° 9: Sueldos

RAMA DE ACTIVIDAD ECONÓMICA: **1.- CONFECCIÓN DE PRENDAS DE VESTIR Y OTRAS MANUFACTURAS TEXTILES**

CARGO / ACTIVIDAD	ESTRUCTURA OCUPACIONAL	COMENTARIOS / DETALLES DEL CARGO O ACTIVIDAD	CÓDIGO IESS FINAL	SALARIO MÍNIMO SECTORIAL 2014

Trabajador de mantenimiento de producción en textiles, cuero y calzado.	C2	Incluye: Mecánico, Electricista, Carpintero, Soldador, Tornero; Otras Manufacturas Textiles	1020000000002	342,14
Diseñador, Dibujante y Elaborador de Moldes.	C3	Incluye: Monta-carguista	1004292603120	341,70
Trabajadores que manejan máquinas sin manipulación de productos químicos / sin riesgo de explosión.	C3	Incluye: Monta-carguista; Otras Manufacturas Textiles	1004292603122	341,70
Bodeguero de confección de prendas de vestir y otras manufacturas textiles	D1		1004292603126	341,29
Trabajador de textiles, cuero y calzado.	E2	Incluye: Ayudante de Bodega, Ayudante en General, Ayudante de Máquinas; Otras Manufacturas Textiles	1020000000001	340,00

Fuente:http://www.jezl-auditores.com/index.php?option=com_content&view=article&catid=55&id=104&Itemid=71

Realizado por: Acuerdo N° MRL-2013-0047

f) Pagos.- Los pagos a proveedores serán distribuidos de la siguiente manera: 40% al contado y 60% a crédito mínimo 90 días.

g) Comisiones en Ventas.- En cuanto a las comisiones en ventas se puede señalar que:

Al por menor: 2% sobre ventas al contado y 1% sobre ventas a crédito.

Al por mayor: 5% sobre ventas totales y si además son al contado en un monto superior a $5000.00 es el 7%.

h) Inventarios.- Como política empresarial se toma como referencia que se espera como inventario final de materia prima un 58% de la producción del mes siguiente.

i) Organización del Trabajo en Producción.- Esta política señala que la producción se da mediante grupos de trabajo establecidos aleatoriamente cada mes y conformado por 7

personas; éstas realizarán el proceso de costura y control de calidad. Para ello se asignarán jefes de grupo quienes anotarán la cantidad de prendas que se obtengan en el mes.

Tabla N° 10

CARACTERÍSTICA DE LA TECNOLOGÍA EN USO

EQUIPOS DE COMPUTO

Nº	**MONITOR**	**IMPRESORA**	**CPU**	**TECLADO**	**MOUSE**
4	SAMSUNG	**MARCA** EPSON LX -300 + **MODELO** P 17 CA **SERIE** ETUY165598	SP GENÉRICO	GENIUS	GENIUS ZCE88B100091
5	GENÉRICO	**MARCA** SAMSUNG **MODELO** SCX-4300 **SERIE** 1456BFG Q8007221	GENIUS	GENIUS	GENIUS
2	LAPTOS	**MARCA** DELL WINDOWS 7 STARTER **MODELO** CM10 **SERIE** X16-960867			
3	INTEL ATOM Dual Core LED	**MARCA** SAMSUNG **MODELO** SCX-4300 **SERIE** 1456BFG Q8007221	ATOM DUAL CORE PROCESADOR INTEL	MULTIMEDIA GENIUS	GENIUS
1	NOTEBOOK	**MARCA** SONY VAIO **SERIE** SVF14415CLB BLACK A10-5745M,6GB,1TB,14" (1A)			
1	MODEM	**MARCA** ECHO LIFEHG5208 **MODELO** HOME GATEWAYS			

Fuente: Datos de la Empresa.

Realizado por: Sandra Valdiviezo.

4.1.2.5. ABREVIATURAS UTILIZADAS EN AUDITORÍA

ABR 1/1

Tabla N° 11: Abreviaturas

ABREVIATURA	SIGNIFICADO
SCVC	Sandra Carolina Valdiviezo Crizón
AP	Archivo Permanente
AC	Archivo Corriente
ABR	Abreviaturas
PA	Programa de Auditoría
PSA	Propuesta de Servicios de Auditoría
EP	Entrevista preliminar
CCI	Cuestionarios de Control Interno
TCCI	Tabulación Cuestionarios de Control Interno
AF	Análisis FODA
IG	Indicadores de Gestión
AS	Análisis Situacional
ECI	Estructura de control Interno
ENC-R	Evaluación del Nivel de confianza y riesgo
ARC	Áreas Críticas
ALC	Alcance de la Auditoría
MP	Memorando de Planificación
HH	Hoja de Hallazgos

Fuente: Procesos de Auditoría

Realizado por: Sandra Valdiviezo.

4.1.2.6. ENTREVISTAS Y VISITAS

En este punto se consideró la evaluación de los cuestionarios de Control Interno según el método COSO II (Anexo 1), aplicados para medir el nivel de confianza y riesgo que mantiene la empresa.

Resultados de la aplicación de la Fórmula para determinar el Nivel de Confianza y Nivel de Riesgo

COMPONENTE 1: Ambiente Interno

Ponderación total de la encuesta

SI =	137
NO =	88

Total = 137+88=225 **Fuente:** (Anexo 3 Componente 1)

$$\textbf{NIVEL DE CONFIANZA} = \frac{\text{CALIFICACIÓN TOTAL}}{\text{PONDERACIÓN TOTAL}}$$

NIVEL DE CONFIANZA = 137/225

NIVEL DE CONFIANZA = 0.61 ⟶ 61%

Tabla Nº 12: Ambiente Interno

← **RIESGO DE CONTROL** →

ALTO	**MODERADO**	**BAJO**
15 – 50 %	51 – 75 %	76 – 95 %
BAJO	**MODERADO**	**ALTO**

← **NIVEL DE CONFIANZA** →

El nivel de confianza obtenido se encuentra en un grado moderado lo que resulta tener también un grado de riesgo de control moderado.

COMPONENTE 2: Establecimiento de Objetivos

Ponderación total de la encuesta

SI =	130
NO =	95

Total = 130+95=225 **Fuente:** (Anexo 3 Componente 2)

$$\textbf{NIVEL DE CONFIANZA} = \frac{\text{CALIFICACIÓN TOTAL}}{\text{PONDERACIÓN TOTAL}}$$

NIVEL DE CONFIANZA = 130/225

NIVEL DE CONFIANZA = 0.58 ⟶ 58%

Tabla Nº 13: Establecimiento de objetivos

RIESGO DE CONTROL

ALTO	**MODERADO**	**BAJO**
15 – 50 %	51 – 75 %	76 – 95 %
BAJO	**MODERADO**	**ALTO**

NIVEL DE CONFIANZA

El nivel de confianza obtenido se encuentra en un grado moderado lo que resulta tener también un grado de riesgo de control moderado.

COMPONENTE 3: Identificación de Riesgos

Ponderación Total de la encuesta

SI =	106
NO =	119

Total = 106+119=225 **Fuente:** (Anexo 3 Componente 3)

$$\textbf{NIVEL DE CONFIANZA} = \frac{\text{CALIFICACIÓN TOTAL}}{\text{PONDERACIÓN TOTAL}}$$

NIVEL DE CONFIANZA = 106/225

NIVEL DE CONFIANZA = 0.47 ⟶ 47%

Tabla Nº 14: Identificación de riesgos

RIESGO DE CONTROL

ALTO	**MODERADO**	**BAJO**
15 – 50 %	51 – 75 %	76 – 95 %
BAJO	**MODERADO**	**ALTO**

NIVEL DE CONFIANZA

El nivel de confianza obtenido se encuentra en un grado bajo, por ende da como resultado un nivel de riesgo de control alto.

COMPONENTE 4: Evaluación de Riesgos

Ponderación Total de la encuesta

SI =	28
NO =	32

Total = 28+32=60 **Fuente:** (Anexo 3 Componente 4)

$$\textbf{NIVEL DE CONFIANZA} = \frac{\text{CALIFICACIÓN TOTAL}}{\text{PONDERACIÓN TOTAL}}$$

NIVEL DE CONFIANZA = 28/60

NIVEL DE CONFIANZA = 0.47 ⟶ 47%

Tabla Nº 15: Evaluación de riesgos

RIESGO DE CONTROL

ALTO	**MODERADO**	**BAJO**
15 – 50 %	51 – 75 %	76 – 95 %
BAJO	**MODERADO**	**ALTO**

NIVEL DE CONFIANZA

El nivel de confianza encontrado es bajo, por lo que resulta un grado de riesgo de control alto.

COMPONENTE 5: Respuesta al Riesgo

Ponderación Total de la encuesta

SI =	38
NO =	37

Total = 38+37=75 **Fuente:** (Anexo 3 Componente 5)

$$\textbf{NIVEL DE CONFIANZA} = \frac{\text{CALIFICACIÓN TOTAL}}{\text{PONDERACIÓN TOTAL}}$$

NIVEL DE CONFIANZA = 38/75

NIVEL DE CONFIANZA = 0.51 ⟶ 51%

Tabla Nº 16: Respuesta al riesgo

RIESGO DE CONTROL

ALTO	**MODERADO**	**BAJO**
15 – 50 %	51 – 75 %	76 – 95 %
BAJO	**MODERADO**	**ALTO**

NIVEL DE CONFIANZA

El nivel de confianza objetivo se encuentra en un grado moderado lo que resulta tener también un grado de riesgo de control moderado.

COMPONENTE 6: Actividades de Control

Ponderación Total de la encuesta

SI =	230
NO =	145

Total = 230+145=375 **Fuente:** (Anexo 3 Componente 6)

$$\textbf{NIVEL DE CONFIANZA} = \frac{\text{CALIFICACIÓN TOTAL}}{\text{PONDERACIÓN TOTAL}}$$

NIVEL DE CONFIANZA = 230/375

NIVEL DE CONFIANZA = 0.61 ⟶ 61%

Tabla Nº 17: Actividades de control

RIESGO DE CONTROL

ALTO	**MODERADO**	**BAJO**
15 – 50 %	51 – 75 %	76 – 95 %
BAJO	**MODERADO**	**ALTO**

NIVEL DE CONFIANZA

El nivel de confianza objetivo se encuentra en un grado moderado, lo que resulta tener también un grado de riesgo de control moderado.

COMPONENTE 7: Información y Comunicación

Ponderación Total de la encuesta

SI =	155
NO =	160

Total = 155+160=315 **Fuente:** (Anexo 3 Componente 7)

$$\textbf{NIVEL DE CONFIANZA} = \frac{\text{CALIFICACIÓN TOTAL}}{\text{PONDERACIÓN TOTAL}}$$

NIVEL DE CONFIANZA = 155/315

NIVEL DE CONFIANZA = 0.49 ⟶ 49%

Tabla Nº 18: Información y comunicación

RIESGO DE CONTROL

ALTO	**MODERADO**	**BAJO**
15 – 50 %	51 – 75 %	76 – 95 %
BAJO	**MODERADO**	**ALTO**

NIVEL DE CONFIANZA

El nivel de confianza obtenido es bajo, por lo que el grado de riesgo de control encontrado es alto.

COMPONENTE 8: Monitoreo

Ponderación Total de la encuesta

SI =	163
NO =	107

Total = 163+107=270 **Fuente:** (Anexo 3 Componente 8)

$$\textbf{NIVEL DE CONFIANZA} = \frac{\text{CALIFICACIÓN TOTAL}}{\text{PONDERACIÓN TOTAL}}$$

NIVEL DE CONFIANZA = 163/270

NIVEL DE CONFIANZA = 0.60 ⟶ 60%

Tabla Nº 19: Monitoreo

RIESGO DE CONTROL

ALTO	**MODERADO**	**BAJO**
15 – 50 %	51 – 75 %	76 – 95 %
BAJO	**MODERADO**	**ALTO**

NIVEL DE CONFIANZA

El nivel de confianza objetivo se encuentra en un grado moderado, lo que resulta tener también un grado de riesgo de control moderado.

4.1.2.7 EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO

Posterior a la aplicación de cuestionario de control interno hemos llegado a las siguientes conclusiones respecto al control interno que se maneja en SUMATEX, bajo los parámetros del método COSO II, que incluye los siguientes componentes:

a) Ambiente Interno

SUMATEX muestra un gran nivel de debilidades en cuanto al correcto desarrollo del ambiente interno, ya que no se ha actualizado los objetivos, misión y visión empresarial; tampoco se ha divulgado ni se ha hecho público los valores éticos que se manejan en la misma y todo esto hace que se trabaje de manera informal y sin fundamento sobre las metas que se deben cumplir en un tiempo determinado. (Anexo 2: Tabulación Componente 1: Ambiente Interno.)

b) Establecimiento de Objetivos

SUMATEX cuenta con objetivos establecidos, pero hace falta mejorarlos, actualizarlos y distribuirlos de forma adecuada, de tal manera que ayuden y aporten al continuo desarrollo de las actividades empresariales. (Anexo 2: Tabulación Componente 2: Establecimiento de objetivos.)

c) Identificación de Riesgos.

En este componente se ha considerado la necesidad de tomar medidas para mejorar el método o sistema de identificación de riesgos, ya que no existe las medidas suficientes para identificar los verdaderos riesgos, sean estos relevantes o no, ante el cuidado de los recursos de la empresa; y, más aún, de los recursos informáticos, ya que de estos depende mucho el desarrollo de SUMATEX. (Anexo 2: Tabulación Componente 3: Identificación de Riesgos.)

d) Evaluación de Riesgos.

Hay mucho por hacer para la mejora de la evaluación de los riesgos en Sumatex, pues se han evidenciado muchas falencias en cuanto a medir el grado de perjuicio de tales riesgos, los daños que pueden ocasionar, y la concurrencia con los que se puedan presentar, por lo que se

hace necesaria la aplicación de métodos de evaluación para brindar opciones para la mejor toma de decisiones. (Anexo 2: Tabulación Componente 4: Evaluación de Riesgos.)

e) Respuesta al Riesgo.

SUMATEX si ha dado respuesta a los riesgos que se han identificado, pero le falta mucho por identificar y aún más, dar respuesta a los mismos para continuar con el normal desarrollo de las operaciones y actividades a las que se dedica la empresa. (Anexo 2: Tabulación Componente 5: Respuesta al Riesgo.)

f) Actividades de Control.

Las actividades de control existentes si han ayudado a la mejora de las operaciones, pero hace falta mejorar aún más para que continúe el desarrollo de la empresa, ya que es de suma importancia implementar actividades que aporten al control y buen desarrollo de las mismas. (Anexo 2: Tabulación Componente 6: Actividades de Control.)

g) Información y Comunicación

Es necesario realizar un análisis de las debilidades y falencias que tienen los métodos de información y comunicación de SUMATEX, para así brindar una opinión adecuada para la mejor toma de decisiones, con lo que se espera mejorar el liderazgo de los administrativos, el desempeño de los empleados y la conformidad de los usuarios externos. (Anexo 2: Tabulación Componente 7: Información y Comunicación.)

h) Monitoreo

SUMATEX mantiene controles y registro de las actividades y operaciones que se realizan, pero es necesaria la mejora continua de éstos, ya que las medidas de control no siempre van a resultar eficientes ante los cambios constantes del medio. (Anexo 2: Tabulación Componente 8: Monitoreo.)

4.1.2.8 DETERMINACIÓN DE ÁREAS CRÍTICAS

ÁREAS CRÍTICAS

ARC 1/1

ORGANIZACIÓN AUDITADA: SUMATEX

Prioridad	Área o Actividad Crítica	Razones
1	Departamento Administrativo.	Falta de gestión direccionada a la seguridad informática.
2	Departamento Informático con escazas normas de seguridad informática.	Poco control y evaluación de los riesgos informáticos. Falta de medidas de seguridad.
3	Área contable y de ventas.	No se toman medidas de cuidado de los equipos informáticos.
4	Información y Comunicación.	Poca fluidez de información oportuna para la adecuada identificación de necesidades y mejor toma de decisiones.

Elaborado por:	Sandra C. Valdiviezo
Fecha:	14/03/2014

ALC 1/2

4.1.2.9 DETERMINACIÓN DEL ALCANCE DE AUDITORÍA

La presente "Auditoría de Seguridad Física y Lógica de Sistemas Informáticos de la Empresa SUMATEX", está orientada a la revisión del control interno del Departamento Informático y de los equipos que maneja esta empresa.

El alcance de la auditoría comprendió:

ALC 2/2

1. Evaluación de la dirección de informática en lo que corresponde a:

- Su organización.
- Funciones.
- Objetivos.
- Estructura.
- Recursos Humanos.
- Normas y Políticas.
- Capacitación.
- Planes de trabajo.
- Controles.
- Condiciones de trabajo.

2. Evaluación de seguridades Físicas y Lógicas.

- Seguridad lógica de los sistemas, confidencialidad y respaldos.
- Identificación de los riesgos.
- Evaluación de los riesgos.
- Seguridades físicas
- Seguridad en el personal
- Seguridad contra virus
- Seguridad en la utilización de los equipos.
- Seguridad en la restauración de los equipos y de los sistemas.
- Plan de contingencia y procedimiento en caso de desastre.

3. Elaboración de informes con inclusión de conclusiones y recomendaciones por cada uno de los trabajos señalados anteriormente.

SUMATEX

AC

Auditoría de Seguridad Física y Lógica de los Sistemas Informáticos.

Del 01 de Enero al 31 de Diciembre del 2012

ARCHIVO CORRIENTE

Elaborado por:	Inicio	Finalización
SCVC	27/03/2014	16/01/2014

4.1.2.10 PROGRAMA DE AUDITORÍA

P.A. 1/2

PROGRAMA DE AUDITORÍA

ORGANISMO: SUMATEX

Hoja Núm.: 1 De: 1

Fecha de formulación: 28/03/2014

FASE	DESCRIPCIÓN	ACTIVIDAD	N°. DE PERSONAL	PERÍODO ESTIMADO		DÍAS ESTABLECIDOS
				Inicio	Término	
Objetivo	Obtener y recopilar información	Obtener evidencia suficiente, competente, relevante y pertinente que permita conocer la situación de SUMATEX. Recopilar la Información necesaria y suficiente para efectuar la auditoría.	1	27/11/2013	13/12/2013	13
Planeación	Conocer la empresa y su estructura funcional y organizacional para dar paso con la auditoría.	Realizar la entrevista al Gerente para obtener información general sobre la entidad.	2	16/12/2013	02/01/2014	17
		Realizar la carta a gerencia, con el fin de dar a conocer el trabajo a realizarse.	1	03/01/2014	07/01/2014	3
		Efectuar una revisión de la estructura orgánica de la entidad para conocer como está dividida la misma.	1	08/01/2014	16/01/2014	7

P.A. 2/2

Evaluación de Control Interno	Evaluar el sistema de control interno existente en SUMATEX.	Aplicar Cuestionarios de Control Interno.	1	17/01/2014	04/02/2014	13
		Evaluar el control interno según los componentes de COSO II.	1	05/02/2014	07/03/2014	23
		Determinar las áreas críticas y hallazgos.	1	10/03/2014	20/03/2014	9
Comunicación de resultados	Dar a conocer los hallazgos encontrados durante la aplicación de la auditoría.	Redactar el borrador del informe final.	1	21/03/2014	21/03/2014	1
		Discuta el borrador del informe con la gerencia y el personal involucrado.	1	25/03/2014	25/03/2014	1
		Elaborar el acta de la lectura del borrador del informe.	1	26/03/2014	26/03/2014	1
		Elaborar el informe final de auditoría realizada a la empresa SUMATEX.	1	27/03/2014	27/03/2014	2

Elaborado por:	Sandra C. Valdiviezo
Fecha:	01/12/2013

MP 1/9

4.1.3 MEMORANDO DE PLANIFICACIÓN

DEFINICIÓN DEL TRABAJO DE AUDITORÍA Y SUS OBJETIVOS

a) Objetivo General

La Auditoría de la seguridad física y lógica de sistemas informáticos tiene como objetivo evaluar el grado de protección del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los albergan. Como auditor informático debí contemplar situaciones como: incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc., que pueden afectar la protección de los recursos informáticos de SUMATEX, e impedir a la vez el cumplimiento de los objetivos organizacionales.

b) Objetivos Específicos

- Evaluar la seguridad en el uso de software la protección de los datos, procesos y programas, así como la seguridad del acceso ordenado y autorizado de los usuarios a la información.
- Identificar que no existan copias piratas, o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión de virus.
- Determinar el nivel de seguridad de la infraestructura informática de SUMATEX, tomando como vectores de ataque aquellos que puedan ser iniciados dentro de la empresa.
- Emitir una opinión clara y concisa sobre la situación actual de la empresa y emitir las recomendaciones apropiadas que permitan a los directivos tomar mejores decisiones.

c) Auditoría de Seguridad Física y Lógica

Esta Auditoría tiene como finalidad la identificación de los riesgos de los sistemas de información que pudieran afectar al cumplimiento de la legalidad vigente, la eficiencia y la eficacia de los procesos soportados por los sistemas de información, en especial los de la administración electrónica manejada a través del sistema SSiAM.

MP 2/9

Para la realización de la auditoría se realizó el estudio previo de la información que contienen los archivos propios de la empresa, el que fue incluido dentro de la Planificación preliminar; asimismo se determinaron áreas críticas, se evaluaron los riesgos, se aplicaron los papeles de trabajo y se emitió el correspondiente informe de auditoría como un aporte para la mejor toma de decisiones.

d) CONOCIMIENTO DE LA EMPRESA

SUMATEX se inicia el 3 de septiembre de 1986, en primera instancia como suministradora de materiales textiles, y luego en el año 1994 incursiona en la confección de prendas blancas como: sábanas, mantelería, prendas de dormir, entre otros; con apenas un par de máquinas industriales adquiridas al remate en el Banco Nacional de Fomento.

Actualmente la empresa cuenta con una fábrica industrial, tres puntos de venta propios ubicados en al Guayaquil 22- 02 y Espejo; en las calles Guayaquil entre colon y Larrea y en las calles Junín 25-35 y Palmeras.

e) MISIÓN

"La Misión de SUMATEX es confeccionar y comercializar prendas de vestir, de dormir y ropa blanca, que satisfagan necesidades del mercado en forma competitiva, cumpliendo con ética las obligaciones con sus clientes, proveedores, empleados, socios, el Estado y la comunidad en la que se desarrollan las actividades de la empresa"

f) VISIÓN

"Ser empresa líder del centro del país en la producción e innovación de prendas de vestir para dormir, así como ser modelo de excelencia en todos sus procesos, reflejada en productos competitivos con fidelidad a sus valores corporativos"

MP 3/9

g) ESTRUCTURA ORGANIZACIONAL

La estructura organizacional de la fábrica SUMATEX es relativamente sencilla con flujo de información de doble vía (ascendente y descendente), con tres niveles jerárquicos, distribuidos en las siguientes áreas funcionales:

- El Área de Producción con las unidades operativas de corte, confección y de acabado
- El Área Administrativa – Financiera con los Dptos. De Gestión, Contable e Informático.
- El Área de Mercadeo y Ventas con sus almacenes 1, 2, y 3.
- El Área de Almacenamiento con sus unidades operativas de archivo y bodega.
- El Área de Producción.
- El Área Administrativa-Financiera.
- El Área de Mercadeo y Ventas.
- El Área de Almacenamiento.

h) FUNCIONARIOS PRINCIPALES

Gerente General:	Ing. Elsa Susana Guaraca Matute
Contadora:	Ing. Paulina Ayala
Consultor Productivo:	Ing. Andrés Posada Hernández.
Supervisor Informático:	Ing. Pablo Cruz.
Jefe de Producción:	Srta. Nancy Saca.
Jefe de Bodegas:	Srta. María Pilco.
Supervisor de Ventas:	Sra. Margarita Muñoz

i) DATOS GENERALES

Logo:

Nombre Empresa: SUMATEX

Representante Legal: Ing. Susana Guaraca

RUC: 1500317605001

Tipo De Contribuyente: Obligado a llevar contabilidad

Planta Industrial: Junín 45-37 y Las Palmeras

Teléfono: (03)2960192

Calificación Artesanal: Junta de Defensa del Artesano Nº 82908

Rama Artesanal: Corte y confección.

Correo: sumatexsg@hotmail.com

Actividades:

- **Actividad Económica Principal**

  Fabricación de prendas de vestir para dormir de: damas, caballeros y niños.

- **Actividades Económicas Secundarias**

  Fabricación de: ropa blanca, edredones, sábanas, ropa de baño, etc.

j) DATOS EMPRESARIALES

Matriz: Riobamba- Guayaquil 22-02 y Espejo

Sucursales: Riobamba - España 20-39 y Guayaquil

Riobamba - 10 de Agosto s/n y Rocafuerte

Distribuidora: Riobamba - Junín y Palmeras.

Nº de empleados: Producción: 27 empleados

Personal Administrativo: 7 personas

Personal de Ventas: 8 personas

Personal bodegas: 3 personas

k) Indicadores de Gestión

INDICADORES DE GESTIÓN INFORMÁTICA		
ACTIVIDAD	**ASUNTO**	**FORMULA**
Costo	Costo de informática en relación al costo administrativo.	Costo Total de informática / Costo total de administración.
	Costo de informática en relación al ingreso de la empresa.	Costo Total de informática / Ingresos totales de la empresa.
	Costo de informática por empleado.	Costo Total de Informática / Número Total de empleados.
	Costo medio por ordenador (PC).	Costo total de compra y mantenimiento de los PCs / Número de los PCs.
	Costo de mantenimiento.	Costo de mantenimiento informático / Costo total informático.
Incidencias	Incidencias debidas al no respeto de la política informática en relación a las incidencias.	Número de incidencias debidas al no respeto de la política informática / número total de incidencias.

MP 6/9

	Tiempo medio con sistema no disponible.	Tiempo con sistema no disponible / tiempo total operativo.
	Tiempo medio entre fallas.	(tiempo operativo – tiempo no disponible) / Número de fallas.
Infraestructura	Tiempo medio del cambio de los equipos.	Tiempo medio entre la identificación de la necesidad de cambio y el cambio efectivo.
	Número medio de ordenadores PCs por empleados.	Número de PCs / Número de empleados.
	Número medio de impresoras por departamento.	Número de impresoras / Número de departamentos.
RRHH	Tiempo dedicado a actividades informáticas innovadoras.	Tiempo dedicado a actividades innovadoras / Tiempo de trabajo total en informática.
	Formación.	Número de horas de formación / número de empleados en informática.
	Nómina de sueldos.	Nómina de sueldos informática / Total Nómina de sueldos.
	Estabilidad.	Número de empleados presentados después de 6 meses / Número de nuevos empleados contratados hace 15 meses.
		Edad media de los empleados.

MP 7/9

Seguridad	Seguridad Lógica.	Nº de incidencias/solicitudes atendidas en un mes
		Tiempo a utilizarse
		Número de incidencias atendidas / número de incidencias recibidas.
	Seguridad Física.	Riesgos identificados / posibles riesgos.
		Número de medidas de seguridad tomadas / posibles medidas de seguridad existentes.
		Número de accesos de personal desautorizados / Número de control de acceso a los equipos informáticos.

l) Actividades de Control Realizadas

Para la evaluación del sistema de control interno existente en la empresa SUMATEX se realizaron cuestionarios de control interno basados en los componentes del COSO II, los cuales permitieron tener un enfoque del nivel de control que tienen, y lo que hace falta mejorar en la empresa según los distintos componentes, como son: ambiente de control, establecimiento de objetivos, identificación de riesgos, evaluación de riesgos, respuesta a los riesgos, actividades de control, información, comunicación y monitoreo.

Igualmente a través de estas evaluaciones se han determinado los niveles de confianza y de riesgo de control que prevalecen en el período examinado; las mismas que fueron revisadas anteriormente.

MP 8/9

m) Determinación de Áreas Críticas

ÁREAS CRÍTICAS

	ORGANIZACIÓN AUDITADA: SUMATEX

Prioridad	Área O Actividad Critica	Razones
1	Departamento Administrativo.	Falta de gestión direccionada a la seguridad informática.
2	Departamento Informático con escazas normas de seguridad informática.	Poco control y evaluación de los riesgos informáticos. Falta de medidas de seguridad físicas y lógicas.
3	Área contable y de ventas.	No resguardan medidas de cuidado de los equipos informáticos.
4	Información y Comunicación.	Poca fluidez de información oportuna para la adecuada identificación de necesidades y mejor toma de decisiones.

Elaborado por:	SCVC
Fecha:	14/03/2014

MP 9/9

n) Determinación del Alcance de Auditoría

La presente "Auditoría de Seguridad Física y Lógica de Sistemas Informáticos de la Empresa SUMATEX", está orientada a la revisión del control interno informático del Departamento Informático y de los equipos que maneja esta empresa.

o) Recursos a utilizar

Económicos	**Valor Total**	**Tecnológicos**	**Valor Total**
Impresiones	$ 50.00	Internet.	$ 90.00
Copias	$ 20.00	Mantenimiento de Laptop.	$ 15.00
Pasajes	$ 25.00		
Gastos Varios	$ 30.00		
TOTAL	**$ 125.00**	**TOTAL**	**$ 105.00**

4.1.4. CARTA A GERENCIA

(Propuesta de Servicios de Auditoría de Seguridad Física y Lógica de Sistemas Informáticos).

I. Antecedentes

SUMATEX se inició el 3 de septiembre de 1986. Estableciéndose legalmente en la ciudad de Riobamba en el año 2007, teniendo como principal actividad comercial la fabricación de ropa deportiva, ropa blanca, prendas de vestir para dormir, trabajo, uniformes, y la comercialización de las mismas a nivel local y nacional.

SUMATEX mantiene un registro continuo de las operaciones contables y de control de inventarios a través de programas informáticos muy poco seguros, los cuales resultan ser un posible blanco fácil para el espionaje, perdidas de información, fraudes, errores, alteraciones, riesgos que deben ser considerados en la toma de decisiones.

El avance de la informática, los sistemas, las telecomunicaciones, y otras aplicaciones de tecnología, han hecho que la empresa SUMATEX tenga que adaptarse rápidamente a los cambios en todos los sentidos, en especial en el giro del negocio, el cual está íntimamente relacionado con la tecnología de la información en el desarrollo de los diferentes procesos empresariales.

II. Objetivos de la Auditoría de Seguridad Física y Lógica de Sistemas Informáticos

Objetivo General

La Auditoría de la seguridad física y lógica de sistemas informáticos tiene como objetivo evaluar el grado de protección del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los albergan. El auditor informático debe contemplar situaciones de incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc., que puedan afectar la protección de los recursos informáticos de SUMATEX, o pueda impedir el cumplimiento de los objetivos organizacionales.

P.S.A 2/11

OBJETIVOS ESPECIFICOS

- Evaluar la seguridad en el uso de software la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.
- Identificar que no existan copias piratas, o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión de virus.
- Determinar el nivel de seguridad de la infraestructura informática de SUMATEX, tomando como vectores de ataque aquellos que puedan ser iniciados dentro de la empresa.
- Emitir una opinión clara y concisa sobre la situación actual de la empresa y emitir las recomendaciones apropiadas que permitan a los dirigentes tomar mejores decisiones.

III. Alcances del Proyecto

El alcance del proyecto comprende:

1. Evaluación de la dirección de informática en lo correspondiente a:

- Su organización.
- Funciones.
- Objetivos.
- Estructura.
- Recursos Humanos.
- Normas y Políticas.
- Capacitación.
- Planes de trabajo.
- Controles.
- Condiciones de trabajo.

2. Evaluación de seguridades Físicas y Lógicas.

- Seguridad lógica de los sistemas, confidencialidad y respaldos.
- Identificación de los riesgos.

- Evaluación de los riesgos.
- Seguridades físicas
- Seguridad en el personal
- Seguridad contra virus
- Seguridad en la utilización de los equipos.
- Seguridad en la restauración de los equipos y de los sistemas.
- Plan de contingencia y procedimiento en caso de desastre.

3. Elaboración de informes que contengan conclusiones y recomendaciones por cada uno de los trabajos señalados anteriormente.

IV. Metodología

La metodología de investigación utilizada en el examen de auditoría fue la siguiente:

1. Para la evaluación de la dirección de informática se llevaron a cabo las siguientes actividades:

- Solicitud de los manuales administrativos, organización, funciones, planes, políticas, estándares utilizados y programas de trabajo.
- Solicitud de costos y presupuestos de informática.
- Elaboración de una entrevista preliminar que permita evaluar a la Dirección.
- Aplicación del cuestionario al personal, y realización de entrevistas.
- Entrevista a líderes de departamentos y a usuarios más relevantes de la dirección de informática.
- Análisis y evaluación de la información.
- Elaboración del informe.

2. Para la evaluación de los sistemas de seguridades físicas y lógicas informáticos se llevaron a cabo las siguientes actividades:

- Aplicación de Indicadores de Gestión Informática.
- Evaluación de plan de contingencia y recuperación en casos de desastre.
- Análisis de la seguridad lógica y confidencial.
- Evaluación de controles a través de lista de chequeos.
- Entrevistas con usuarios de los sistemas.
- Evaluación directa de la información obtenida contra las necesidades y requerimientos de los usuarios.
- Análisis objetivo de la estructuración y flujo de los programas.
- Análisis y evaluación de la información compilada.
- Elaboración del informe.

3. Para la evaluación de los equipos se llevaron a cabo las siguientes actividades:

- Elaboración de un cuestionario sobre la utilización de equipos, archivos, unidades de entrada/salida, equipos periféricos, y su seguridad.
- Visita a las instalaciones y a los lugares de almacenamiento de archivos magnéticos.
- Visita técnica de comprobación de seguridad física y lógica de las instalaciones.
- Evaluación de los sistemas de seguridad de acceso.
- Evaluación de la información recopilada, obtención de gráficas, porcentajes de utilización de los equipos y su justificación.
- Determinación de áreas críticas.
- Análisis de niveles de confianza y de riesgo.
- Determinación de hallazgos.
- Elaboración del informe.

3. Elaboración del informe final, presentación y discusión del mismo, y presentación de conclusiones y recomendaciones.

P.S.A 5/11

V. Tiempo y Costo

Etapa	Tiempo
Planificación • Preliminar • Específica	 25 Días 15 Días
Ejecución	45 Días
Comunicación de Resultados	5 Días
Total de Auditoría	**3 meses**

Etapa	Costo
Planificación • Preliminar • Específica	 $ 250.00 $ 250.00
Ejecución	$480.00
Comunicación de Resultados	$ 220.00
Total de Auditoría	**$ 1,200.00**

VI Contrato de Prestación de Servicios Profesionales

En la ciudad de Riobamba, provincia de Chimborazo, a los tres días del mes de Enero del 2014, por una parte la Empresa SUMATEX, representado por la Ing. Elsa Susana Guaraca Matute, en su condición de Gerente – Propietaria, y que en lo sucesivo se denominará "cliente"; y, por otra parte la Ing. Carolina Valdiviezo Crizón, quién en adelante se denomina "la auditora", convienen en celebrar el presente contrato de prestación de servicios profesionales para la ejecución de una Auditoría de Seguridad Física y Lógica de Sistemas Informáticos, de conformidad con las siguientes declaraciones y clausulas:

DECLARACIONES

I. El cliente declara:

a) Que es una empresa productora y comercializadora de ropa y varios textiles.

b) Que está representado para este acto por la Ing. Esla Susana Guaraca Matute y que tiene como su domicilio las calles Junín 45-37 y Palmeras.

c) Que requiere obtener servicios de auditoría de seguridad física y lógica de sistemas informáticos, por lo que ha decidido contratar los servicios de la auditora.

II. Por su parte la Auditora declara:

a) Que es un Contador y Auditor Independiente, legalmente inscrito y existente de acuerdo con las leyes y normativas vigentes, facultado para prestar servicios de auditoría de seguridad física y lógica de sistemas informáticos a la empresa SUMATEX, que actúa como persona natural obligada a llevar contabilidad.

b) Que señala como su domicilio las calles Rio Quinindé y Río Amazonas Mz. B Lote #3 de la Cooperativa de Vivienda Ecuacerámica.

III. Declaran ambas partes:

a) Que habiendo llegado a un acuerdo en las declaraciones antes mencionadas, lo formalizan emitiendo el presente contrato, bajo las siguientes cláusulas:

Primera. Objeto

La auditora se obliga a prestar al cliente los servicios de auditoría en informática para llevar a cabo la evaluación de la dirección de informática, cuyos términos se detallan en la propuesta de servicios anexa que, firmada por las partes, forma parte integrante del contrato.

Segunda. Alcance del trabajo

El alcance de los trabajos que llevará a cabo el auditor interno dentro de este contrato son:

a) Evaluación de la dirección de informática en lo que corresponde a:

- Su organización.
- Funciones.
- Objetivos.
- Estructura.
- Recursos Humanos.
- Normas y Políticas.
- Capacitación.
- Planes de trabajo.
- Controles.
- Condiciones de trabajo.

b) Evaluación de seguridades Físicas y Lógicas.

- Seguridad lógica de los sistemas, confidencialidad y respaldos.
- Identificación de los riesgos.
- Evaluación de los riesgos.
- Seguridades físicas.
- Seguridad en el personal.
- Seguridad contra virus.
- Seguridad en la utilización de los equipos.
- Seguridad en la restauración de los equipos y de los sistemas.

- Plan de contingencia y procedimiento en caso de desastre.
- Elaboración de informes que contengan conclusiones y recomendaciones por cada uno de los trabajos señalados en los incisos **a** y **b** de esta cláusula.

Tercera. Programa de trabajo

El cliente y el auditor convienen en desarrollar de forma conjunta un programa de trabajo en el que se determinen con precisión: las actividades a realizar por cada una de las partes, los responsables de llevarlas a cabo y las fechas de su realización.

Cuarta. Supervisión

El cliente o quien designare éste, tendrá derecho a supervisar los trabajos que se le han encomendado al auditor dentro de este contrato y a dar por escrito las instrucciones que estime convenientes.

Quinta. Coordinación de los trabajos

El cliente (Empresa) designará a un coordinador del proyecto, quien será el responsable de coordinar la recopilación de la información que solicite el auditor, y de que las reuniones y entrevistas establecidas en el programa de trabajo se lleven a cabo en las fechas establecidas.

Sexta. Horario de trabajo

El auditor dedicará el tiempo necesario para cumplir satisfactoriamente con los trabajos materia de la celebración de este contrato, de acuerdo al programa de trabajo convenido por ambas partes, y gozará de libertad fuera del tiempo destinado al cumplimiento de las actividades, por lo que no estará sujeto a horarios y jornadas determinadas.

Séptima. Personal asignado

El auditor designará para el desarrollo de los trabajos objeto de este contrato a socios del despacho, a quienes incorporará en el número que se requieran y de acuerdo a los trabajos a realizar.

Octava. Relación laboral

La auditora no tendrá ninguna relación laboral directa con el cliente, ni tampoco el personal que ocupe ésta para dar cumplimiento con las obligaciones del presente contrato, por lo que exime al cliente de cualquier responsabilidad que a este respecto existiere.

Novena. Plazo de trabajo

El auditor se obliga a terminar los trabajos señalados en la cláusula segunda de este contrato en 90 días hábiles a partir de la fecha de la firma de este contrato y del cobro del anticipo correspondiente. El tiempo estimado para la terminación de los trabajos está con relación a la oportunidad con que el cliente entregue los documentos requeridos por el auditor y, al cumplimiento de las fechas estipuladas en el programa de trabajo aprobado por las partes, por lo que cualquier retraso ocasionado por parte del personal del cliente o de usuarios de los sistemas repercutirá en el plazo estipulado, el cual deberá incrementarse de acuerdo a las nuevas fechas establecidas en el programa de trabajo, sin perjuicio alguno para el auditor.

Décimo. Honorarios

El cliente pagará al auditor por los trabajos objeto del presente contrato, honorarios por la cantidad de $1,200.00 más el impuesto al valor agregado correspondiente. La forma de pago será la siguiente:

a) 40% a la firma del contrato.
b) 20% a los 30 días hábiles después de iniciados los trabajos.
c) 40% a la terminación de los trabajos y presentación del informe final.

Undécima. Alcance de los honorarios

El importe señalado en la cláusula décima compensará el auditor por: sueldos, honorarios, organización y dirección técnica propia de los servicios de auditoría, a excepción de los gastos de realización mencionados anteriormente, los que serán asumidos por la empresa.

Duodécima. Incremento de honorarios

En caso de que se tenga un retraso debido a la falta de entrega oportuna de información, demora o cancelación de las reuniones, o cualquier otra causa imputable al cliente, este contrato se incrementará en forma proporcional al retraso y se señalará el incremento de común acuerdo.

Decimotercera. Trabajos adicionales

De ser necesaria alguna adición a los alcances o productos del presente contrato, las partes celebrarán por separado un adendum que formará parte integrante de este instrumento y en forma conjunta se acordará el nuevo costo.

Decimocuarta. Viáticos y pasajes

El importe de los viáticos y pasajes en que incurra el auditor en el traslado, hospedaje y alimentación que requiera durante su permanencia en la ciudad de Riobamba como consecuencia de los trabajos objeto de este contrato, será por cuenta del cliente.

Decimoquinta. Gastos Generales

Los gastos de fotocopiado y dibujo que se produzcan con motivo de este contrato correrán por cuenta del cliente.

Decimosexta. Causas de rescisión

Serán causa de rescisión del presente contrato la violación o incumplimiento de cualquiera de las cláusulas anteriores de este contrato.

Decimoséptima. Jurisdicción

Todo lo no previsto en este contrato se regirá por las disposiciones relativas, contenidas en el Código Civil del Ecuador y, en caso de controversia para su interpretación y cumplimiento, las partes se someten a la jurisdicción de los tribunales de justicia de la ciudad de Riobamba, renunciando al fuero que les pueda corresponder en razón de su domicilio presente y futuro.

Enteradas las partes del contenido y alcance legal de este contrato, lo rubrican y firman de mutuo acuerdo, en original y tres copias.

Dado y firmado en la ciudad de Riobamba, el día 03 de Enero del 2014.

EL CLIENTE

EL AUDITOR

4.2. EJECUCIÓN DE LA AUDITORÍA

4.2.1. Recopilación de Información

4.2.1.1 Obtención de Evidencias

En este punto fue necesario considerar la obtención de información y recopilación de evidencias suficientes y confiables que permita determinar la validez de los mismos, a la vez que reflejen la realidad de la organización y permitan establecer los hallazgos. Esta evidencia debió ser obtenida bajo el sistema de control interno, enfocándonos en la seguridad física y lógica de los sistemas informáticos.

Tabla Nº 20

MATRIZ DE EVIDENCIAS

Componente	**Evidencia**	**Análisis**
Actividades de Control	Medidas de seguridad	Las medidas de control

Seguridad Física	físicas incompletas. Instalaciones eléctricas seguras. Actividades de control poco frecuentes. Falta de medidas de restricción del personal a departamentos donde funcionan los sistemas informáticos. Existe una sola persona responsable del cuidado de todos los equipos informáticos. Falta de medidas preventivas y contingentes. No se ha implementado medidas de seguridad industrial. Las medidas de seguridad implantadas en la empresa no son de conocimiento general.	interno y seguridad que tiene implementado SUMATEX son buenas, pero a la vez son demasiado básicas, ya que existen también algunos medidas que se deberían adoptar en la empresa para que se pueda mantener la confiabilidad y seguridad de los recursos informáticos.
Actividades de Control Seguridad Lógica	Escaso control de accesos de virus, hackers, y otros que afecten al software de los equipos. Se mantienen soportes de información solamente internos, más no externos.	El manejo del Software es el apropiado pero se necesita implementar medidas de control y seguridad para que pueda salvaguardar la información de la empresa y sobretodo se pueda aprovechar al máximo sus

	Falta de control en el cumplimiento de políticas informáticas. Inexistencia de control de acceso a páginas web innecesarias.	beneficios.

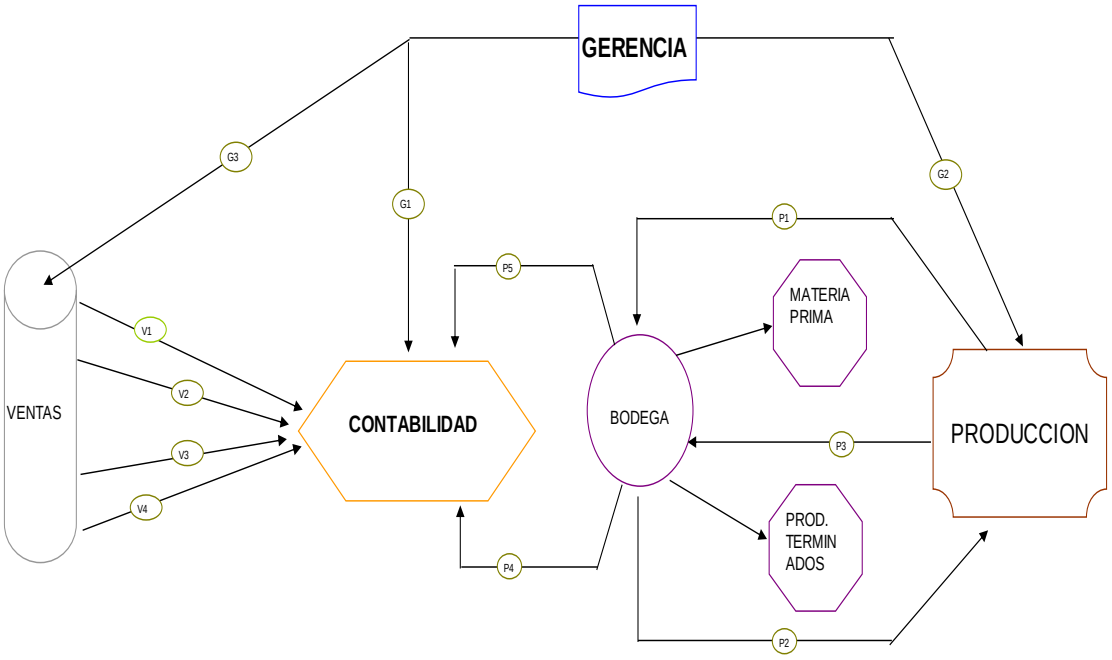
Fuente: Procesos de Auditoría

Realizado por: Sandra Valdiviezo.

Estructura del Sistema de Generación de Reportes y Documentación.

Es esta ilustración se determina el sistema de transferencia de documentos existente que legaliza la autorización de cada proceso.

Ilustración N° 5: Estructura de generación de reportes.



Fuente: Archivo Permanente SUMATEX

Realizado por: Consultor Productivo SUMATEX

4.2.2 EVALUACIONES

4.2.2.1 EVALUACIÓN DE LA ESTRUCTURA ORGÁNICA

Para evaluar la estructura orgánica se solicitó la información referente a:

- Organigramas.
- Funciones.
- Objetivos y Políticas.
- Análisis, Descripción y evaluación de puestos.
- Manual de procedimientos.
- Guías de actividad.

Igualmente, para culminar y llegar más a fondo con el análisis y evaluación se aplicó el siguiente cuestionario considerado como:

ENTREVISTA PRELIMINAR

EP. 1/3

Auditoría de Seguridad Física y Lógica de Sistemas Informáticos

Entidad Evaluada: SUMATEX

Objetivo: *Evaluar de manera general el manejo y desarrollo de la dirección en los ámbitos de la organización.*

1. ¿Se ajusta la estructura orgánica actual a las disposiciones jurídicas vigentes?

SI [__X__] NO [_____] ¿Por qué? _____

Objetivo de la Estructura

4. ¿Permite la estructura organizacional actual que se lleven a cabo con eficiencia:

- Las atribuciones encomendadas? Sí __ No ___
- Las funciones establecidas? Sí __ No ___
- La distribución del trabajo? Sí __ No ___
- El control interno? Sí ___ No ___

EP. 2/3

Niveles Jerárquicos

5. ¿Los niveles jerárquicos establecidos actualmente son necesarios y suficientes para el desarrollo de las actividades del área? Sí ___ No ___

6. ¿Permite los niveles jerárquicos actuales que se desarrolle adecuadamente la:

- Operación? Sí ___ No ___
- Supervisión? Sí ___ No ___
- Control? Sí ___ No ___

7. Considera que algunas áreas debería tener:

- Mayor Jerarquía? Sí ___ No ___
- Menor Jerarquía? Sí ___ No ___

¿Por qué razón? .....

Departamentalización

8. ¿Se consideran adecuados los departamentos, áreas y secciones en que está dividida actualmente la Empresa? Sí ___ No ___ ¿Por qué

9. ¿Las áreas y sus subáreas tienen delimitadas con claridad sus responsabilidades?

Sí ___ No ___

En caso de ser negativa su respuesta: ¿Qué efectos provoca esta situación? .....

Puestos

10. ¿Los puestos actuales son adecuados a las necesidades que tiene cada área para llevar a cabo sus funciones? Sí ___ No ___

11. ¿El número de empleados que trabajan actualmente en cada área son suficientes para cumplir con las funciones encomendadas? Sí ___ No ___

EP. 3/3

12. ¿El número de personas es el adecuado en cada uno de los puestos?

Sí ___ No ___

No, ¿Cuál es el número de personas que consideraría adecuado para cada puesto de Trabajo?

Recursos Humanos

13. ¿Se deja de realizar alguna actividad por falta de personal? Sí ___ No ___

14. ¿Está capacitado el personal para realizar sus funciones con eficiencia?

Sí ___ No ___

15. ¿Es adecuada la calidad del trabajo del personal? Sí ___ No ___

16. ¿Es frecuente la repetición de los trabajos encomendados? Sí ___ No ___

17. ¿El personal es discreto en el manejo de la información confidencial? Sí ___ No ___

18. ¿Acata el personal las políticas, sistemas y procedimientos establecidos?

Sí ___ No ___ ¿Por qué? ……..

19. ¿El personal es comprometido con el cuidado de los recursos informáticos?

Sí _X_ No ___

RESULTADOS DE LA EVALUACIÓN

Objetivo de la Estructura

Es necesario implementar medidas de control interno más adecuadas en la empresa para su cumplimiento y sobre todo para que brinde confianza para el cumplimiento de las metas y objetivos institucionales.

Niveles Jerárquicos

En los niveles Jerárquicos con que cuenta SUMATEX es necesario contratar personal con mayor preparación y capacidad de liderazgo que ayude a exigir el cumplimiento de las medidas de control interno.

Departamentalización

Es necesario implementar un área de control interno que permita el control de los procesos y funciones, velando por una adecuada segregación de funciones, cumplimiento de medidas de seguridad físicas y lógicas de sistemas informáticos y el cuidado de todos los recursos con los que cuenta la empresa.

Puestos

Por el mismo motivo por el que se necesita un área de control interno, también es necesario disponer de una persona que cuenta con la suficiente capacidad intelectual para que ejerza este cargo y ayude a la administración a tomar decisiones adecuadas.

Recursos Humanos

El escaso control en el cumplimiento de las funciones, hace que éstos sean manejados de manera incorrecta sin cumplir con las políticas, objetivos y manuales a causa de la poca comunicación.

4.2.2.2 Evaluación de la Seguridad Física y Lógica

Adicional a la evaluación realizada a través de la aplicación de cuestionarios de Control Interno basados en el método COSO II, se ha utilizado el siguiente check list como método de verificación de medidas de seguridad con que cuenta la empresa:

Tabla Nº 21: Lista de chequeo

Seguridad Física	**Posee**		**Observaciones**
	Si	**No**	
Condiciones climatológicas.	X		Existe una infraestructura adecuada para prevenir daños causados por el

			clima.
Incendios accidentales		X	No posee medidas de seguridad industrial que ayude a prevenir estos riesgos.
Tormentas.	X		
Inundaciones.		X	
Amenazas ocasionadas por el hombre.	X		Son pocas las medidas de seguridad contra la amenaza del hombre que se han implantado.
Sabotajes Internos y externos.		X	Existencia de entorpecimiento intencionado y malicioso por parte del personal de SUMATEX en las actividades de la empresa, en razón de lucha o protesta por inconformidades de los mismos.
Cámaras de seguridad.	X		No son adaptadas para toda la empresa, si no solo para las puertas principales.(exterior)
Malas Instalaciones eléctricas.	X		Posee instalaciones eléctricas adecuadas.
Robo.	X		Ante la ausencia de evidencias no se puede determinar su incidencia.
Fraude.		X	Existencia de fraudes electrónicos por parte de crackers a través de la red.
Utilización de guardias.		X	
Utilización de detectores de metales.		X	
Utilización de sistemas de control biométricos.		X	
Verificación Automática de firmas.		X	

Protección Electrónica.		X	Existencia de: barreras infrarrojas, detectores ultrasónicos, detector de aberturas, vibraciones o rompimiento de vidrios.
Seguridad Lógica	**Aplica**		**Observaciones**
	Si	**No**	
Claves de acceso.	X		No son de uso exclusivo de una sola persona.
Firewall.	X		
Firewalls personales.		X	
Inspección de paquetes		X	
Filtrado de paquetes.		X	
Proxy-gateways de aplicaciones.		X	
Dual- Homed Host.		X	
Screened Host.	X		
Screened Subnet.		X	
Encriptación.	X		
Criptología.		X	
Algoritmo HASH.		X	
Algoritmos Asimétricos.		X	
Contraseñas.	X		
Tarjetas de acceso.		X	
Antivirus.	X		
Firmas digitales.		X	
Copias de seguridad/Backups.	X		
Soportes externos.		X	
Soportes Internos.	X		

Fuente: Procesos de Auditoría

Realizado por: SCVC.

I.G. 1/4

4.2.2.3 Indicadores de Gestión

Cuadro Nº 22

INDICADORES DE GESTIÓN INFORMÁTICA							
Actividad	**Nombre del Indicador**	**Unidad de Medida**	**Fórmula**	**Frecuencia**	**Interpretación**	**Brecha**	**Análisis**
Costo	Costo de informática en relación al costo administrativo.	%	Costo Total de informática / Costo total de administración.	ANUAL	(=) $ 9.643/42.695,54	0.23	Se considera que el 23% de los costos administrativos, son invertido en informática
	Costo de informática en relación a los ingresos de la empresa.	%	Costo Total de informática / Ingresos totales de la empresa.	ANUAL	(=) $ 9.643/447.684,36	0.2	Solo el 20% de los ingresos son invertidos en costos informáticos.
	Costo de informática por empleado.	%	Costo Total de Informática / Número Total de empleados.	ANUAL	(=) $ 9.643/45	214.29	Los costos informáticos son recargados a los empleados en un 214%.
	Costo medio por ordenador (PC).	$	Costo total de compra y mantenimiento de los PC / Número de los PC.	ANUAL	(=) (9643+285)/15	661.87	Se considera que por computador se estima un valor de $ 661 por compra y mantenimiento.

Fuente: Datos de la empresa
Realizado por: SCVC

Costo	Costo de mantenimiento.	%	Costo de mantenimiento informático / Costo Total Informático.	ANUAL	(=)$ 285 / $ 9.643	0.03	El 3% de los costos totales informáticos, son de mantenimiento.
Incidencias	Incidencias debidas al no respeto de la política informática en relación al total de las incidencias.	%	Número de incidencias debidas al no respeto de la política informática / número total de incidencias.	MENSUAL	(=) 53/140	0.38	El 38% de incidencias son debidas al no respeto de las políticas.
	Tiempo medio con sistema no disponible.	%	Tiempo con sistema no disponible / tiempo total operativo.	ANUAL	(=) 192 horas/1960 horas	0.1	El 10% del tiempo trabajado en los S.I. son perdidos.
	Tiempo medio entre fallas.	%	(tiempo operativo – tiempo no disponible) / Número de fallas.	ANUAL	(=) 1960-2/24	81.58	El tiempo desperdiciado es un 81% por fallas.
Infraestructura	Tiempo medio del cambio de los equipos.	%	Tiempo medio entre la identificación de la necesidad de cambio y el cambio efectivo.	DÍA	3 días estimados.		Se toman 3 días en solucionar un problema informático.
	Número medio de ordenadores PC por empleados.	%	Número de PC / Número de empleados.	ANUAL	(=) 15/45	0.33	El 33% de los empleados cuenta con un equipo Inf.

Fuente: Datos de la empresa

Realizado por: SCVC

	Número medio de impresoras por departamento	UND.	Número de impresoras / Número de departamentos.	ANUAL	(=) 16/6	2.67	Por departamento cuentan con 2 impresoras.
RRHH	Tiempo dedicado a actividades informáticas innovadoras	%	Tiempo dedicado a actividades innovadoras / Tiempo de trabajo total en informática.	MENSUAL	(=) 5 horas/40 horas	0.13	Solo el 13% del tiempo es utilizado para actividades innovadoras.
	Formación	%	Número de horas de formación / número de empleados en informática.	MENSUAL	(=) 8 horas al mes/5	1.6	En 1.6 % del tiempo se utiliza para capacitaciones.
	Nómina de sueldos	%	Nómina de sueldos informática / Total Nómina de sueldos.	MENSUAL	(=) (292*5) / (292*45)	0.11	El 11% de los empleados hacen uso de los S.I.
	Estabilidad	%	Número de empleados presentados en enero 2012 / Número de nuevos empleados contratados hasta diciembre 2012.	ANUAL	(=) 45/46	0.98	Se mantiene un 98% de estabilidad en el año.
		AÑOS	Edad media de los empleados.	PARCIAL	(=) (19+43)/2	31	Los empleados tienen una edad media de 31 años.

Fuente: Datos de la empresa

Realizado por: SCVC

I.G. 4/4

Seguridad	Seguridad Lógica.	Unid.	Nº de incidencias / solicitudes atendidas en un mes.	MENSUAL	(=) 5/3	1.67	De cada 5 incidencias presentadas 3 son atendidas.
		%	Número de incidencias atendidas / número de incidencias recibidas.	MENSUAL	(=) 3 / 4	0.75	El 75% de las incidencias recibidas son atendidas.
	Seguridad Física	%	Riesgos identificados / posibles riesgos.	MENSUAL	(=) 5 /15	0.3	Solo el 30% de los riesgos han sido identificados.
		%	Número de medidas de seguridad tomadas / posibles medidas de seguridad existentes.	ANUAL	(=) 11/35	0.31	El 31% de medidas de seguridad existentes han sido tomadas.
		%	Número de accesos de personal desautorizados / Número de control de acceso a los equipos informáticos.	MENSUAL	(=) 4 /2	2	Existen más de 2 accesos desautorizados a los equipos informáticos al mes.

Fuente: Datos de la empresa

Realizado por: SCVC

4.2.2.4 Matriz De Control de Áreas Críticas

Análisis realizado de acuerdo a la evaluación de los componentes del COSO II.

ÁREAS CRÍTICAS

ARC 1/8

ORGANIZACIÓN AUDITADA: SUMATEX

COMPONENTE: AMBIENTE INTERNO

ACTIVIDAD: CUIDADO DE LOS RECURSOS INFORMÁTICOS.

Prioridad	Descripción
1	El ambiente Interno de SUMATEX es bueno, pero no tiene la cultura empresarial necesaria para incentivar al personal a cuidar los recursos de la empresa y sobre todo los recursos informáticos, ya que estos representan un punto importante e indispensable para el desarrollo eficiente de las actividades.
2	La misión y visión institucional deben ser actualizadas de acuerdo a los avances y desarrollo de las actividades económicas de la empresa y del país; y en este caso del avance tecnológico del entorno.

Elaborado por:	SCVC
Fecha:	10/02/2014

ÁREAS CRÍTICAS

ARC 2/8

ORGANIZACIÓN AUDITADA: SUMATEX

COMPONENTE: ESTABLECIMIENTO DE OBJETIVOS

ACTIVIDAD: OBJETIVOS ENFOCADOS EN LA SEGURIDAD INFORMÁTICA.

Prioridad	Descripción
1	SUMATEX tiene establecidos objetivos encaminados a la gestión informática pero estos no abarcan la seguridad física y lógica de los sistemas informáticos.
2	Los objetivos deben ser planteados nuevamente y actualizados de acuerdo al cumplimiento y avance de los que han sido planteados anteriormente.

Elaborado por:	SCVC
Fecha:	10/02/2014

ÁREAS CRÍTICAS

ARC 3/8

ORGANIZACIÓN AUDITADA: SUMATEX

COMPONENTE: IDENTIFICACIÓN DE RIESGOS

ACTIVIDAD: MÉTODOS PARA IDENTIFIAR RIESGOS

Prioridad	Descripción
1	SUMATEX no ha realizado un análisis profundo de los posibles riesgos a los que se puede enfrentar la empresa y sobre todo a los riesgos que amenazan el normal funcionamiento de los equipos informáticos.
2	No se tiene una idea clara del grado de perjuicio que pueden producir los riesgos.

Elaborado por:	SCVC
Fecha:	11/02/2014

ÁREAS CRÍTICAS

ARC 4/8

ORGANIZACIÓN AUDITADA: SUMATEX

COMPONENTE: EVALUACIÓN DE RIESGOS

ACTIVIDAD: LOS RIESGOS IDENTIFICADOS SON PERJUDICIALES

Prioridad	Descripción
1	Todos los riesgos que se pueden presentar son perjudiciales, pero si existe un rango de los riesgos que pueden causare daños severos a la organización, por lo que se deben realizar el respectivo análisis y evaluación para tomar las medidas correctivas o preventivas correspondientes.

Elaborado por:	SCVC
Fecha:	11/02/2014

ÁREAS CRÍTICAS

ARC 5/8

ORGANIZACIÓN AUDITADA: SUMATEX

COMPONENTE: ACTIVIDADES DE CONTROL "SEGURIDAD FÍSICA"

ACTIVIDAD: NO POSEE ADECUADAS MEDIDAS DE SEGURIDAD FÍSICA.

Prioridad	Descripción
1	SUMATEX cuenta con medidas de seguridad, pero hace falta medidas de Seguridad físicas tales como : • Seguridades Industriales que prevenga incendios. • Medidas de protección ante posibles inundaciones. • Sabotajes internos y externos. • Fraudes. • Utilización de guardias. • Detectores metálicos. • Sistemas biométricos • Verificación automática de firmas • Protección electrónica como: barreras infrarrojas, detectores de aberturas, vibraciones o rompimiento de vidrios, etc.

Elaborado por:	SCVC
Fecha:	12/02/2014

ÁREAS CRÍTICAS

ARC 6/8

ORGANIZACIÓN AUDITADA: SUMATEX

COMPONENTE: ACTIVIDADES DE CONTROL

ACTIVIDAD: NO POSEE ADECUADAS MEDIDAS DE SEGURIDAD LÓGICA

Prioridad	Descripción
1	Es necesario implementar medidas de seguridad lógica en el sistema informático que maneja SUMATEX, que permitan evitar daños o pérdidas; medidas tales como: • Utilización de Firewalls personales. • Inspecciones de paquetes informáticos. • Filtrados de paquetes informáticos. • Utilizar el sistema Proxy - gateways para aplicaciones informáticas. • Aplicar el Dual – Homed Host • Utilizar el Screened Subnet • Aplicar la Criptología • Utilizar el Algoritmo HASH • Considerar la aplicación de Algoritmos asimétricos • Procurar la utilización de Tarjetas de acceso • Aplicar firmas digitales • Utilizar soportes externos de datos.

Elaborado por:	SCVC
Fecha:	12/02/2014

ÁREAS CRÍTICAS

ARC 7/8

ORGANIZACIÓN AUDITADA: SUMATEX

COMPONENTE: INFORMACIÓN Y COMUNICACIÓN

ACTIVIDAD: IMPORTANCIA DE LA INFORMACIÓN

Prioridad	Descripción
1	La comunicación y fluidez de la información son caracteres importantes para el adecuado funcionamiento de la empresa, sean estos en los parámetros de ambiente interno, el establecimiento de objetivos, la identificación de riesgos a los que se enfrente la empresa; ó, el establecimiento de actividades de control para toda la empresa, ya sea de seguridades físicas o lógicas de la información.
2	Un buen liderazgo es necesario para mantener buenas líneas de comunicación y de esta manera identificar las falencias, riesgos y medidas de control que se puedan optar para mantener la seguridad y confianza de la empresa.

Elaborado por:	SCVC
Fecha:	13/02/2014

ÁREAS CRÍTICAS

ARC 8/8

ORGANIZACIÓN AUDITADA:.. SUMATEX

COMPONENTE: MONITOREO

ACTIVIDAD: MEDIDAS DE MONITOREO QUE MANEJA SUMATEX

Prioridad	Descripción
1	No se mantiene un control, ni registro de las actividades que los administradores y usuarios realizan sobre los sistemas informáticos, lo que provoca un nivel de riesgo de control alto y nivel bajo de confianza, pues no se sabe con exactitud quienes hacen uso de los equipos y si éstos están autorizados o no para hacerlo.
2	La eficiencia y desarrollo normal de los equipos no son medidos de manera frecuente.
3	No se mantiene un control adecuado, en el uso de las páginas web, para evitar que estas sean utilizadas de manera innecesaria.

Elaborado por:	SCVC
Fecha:	16/02/2014

4.2.3. DETERMINACIÓN DE HALLAZGOS

H.H. 1/5

Folio 1

AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA DE SISTEMAS INFORMÁTICOS

DESARROLLO DE HALLAZGOS

1	**ORGANIZACIÓN AUDITADA:** SUMATEX

2	**PROGRAMA:** Planeación	**ACTIVIDAD:** Entrevista preliminar.

3	**HALLAZGO:** No se han establecidos objetivos y políticas de seguridad informática.

4	**CONDICIÓN:** No están establecidos objetivos que se enfoquen en el cuidado de la seguridad informática, mucho menos políticas que se deban aplicar en los procesos realizados por el personal.

5	**CRITERIO:** Las empresas deben contar con medidas de control interno que salvaguarden los recursos de la misma y brindar confiabilidad a quienes hacen uso de dichos recursos.

6	**CAUSA:** La gestión de los recursos informáticos es muy generalizada y no profundiza en temas de seguridad, tanto del manejo físico como lógico de los

	sistemas informáticos.

7	**EFECTO:** La falta de objetivos y políticas de seguridad informática provoca la inseguridad en la manipulación y conservación de los equipos, confidencialidad de la información, soporte de los datos y salvaguardo de los recursos informáticos.

8	**COMENTARIO:** Toda empresa debe tener especial cuidado de su seguridad informática, ya que la información, el manejo de los equipos informáticos y la tecnología, son medidas de las que depende el continuo desarrollo de las sus actividades y por ende el éxito empresarial.

9	**CONCLUSIONES:** La gestión informática de la empresa SUMATEX debe ir más allá de identificar los riesgos más frecuentes, es decir brindar seguridad en la manipulación, control y manejo de los equipos informáticos y estar en constante monitoreo y evaluación ante posibles riesgos.

10	**RECOMENDACIONES:** La administración y gestión del departamento informático deberá adoptar medidas y políticas que salvaguarden los recursos informáticos, tales como: medidas preventivas, medidas de control y medidas correctivas.

11	**OBSERVACIONES:**

Folio 2

Elaborado por:	SCVC
Fecha:	16/02/2014

Folio 1

H.H. 2/5

AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA DE SISTEMAS INFORMÁTICOS

DESARROLLO DE HALLAZGOS

1	**ORGANIZACIÓN AUDITADA:** SUMATEX

2	**PROGRAMA:** Planeación	**ACTIVIDAD:** Entrevista preliminar.

3	**HALLAZGO:** No se ha designado a un funcionario exclusivo para el manejo responsable de las claves de acceso a los sistemas informáticos.

4	**CONDICIÓN:** No existe un solo funcionario responsable del manejo de las claves de acceso a los sistemas de cada uno de los equipos, realizando esta actividad varias personas, lo cual es un serio riesgo de que se mal utilice la información del sistema administrativo y contable informático.

5	**CRITERIO:** Se deben establecer por escrito las responsabilidades de cada puesto de trabajo, hacerlas conocer a los interesados, de tal forma que exista una adecuada segregación de funciones y deberes, y se guarde la respectiva confidencialidad y sigilo de la información.

6	**CAUSA:** La falta de control interno por parte de la administración del desarrollo de las actividades del personal, y la falta de seguridades y cuidado de la información confidencial.

7	**EFECTO:** El acceso incontrolado al sistema de ventas, compras y control de inventarios por parte de las vendedoras, supervisoras de ventas de cada local de distribución de SUMATEX y de personal ajeno al cargo.

8	**COMENTARIO:** Se debe seleccionar y controlar a los empleados delimitando sus funciones y responsabilidades, de manera que se logre la eficiencia de sus labores y en este caso salvaguardar la seguridad y confianza en el manejo de la información.

9	**CONCLUSIONES:** La inexistencia de un adecuado control y la ineficiente segregación de funciones, provoca la inseguridad en la difusión de la información, el incorrecto uso del sistema y el inadecuado salvaguardo de los recursos.

10	**RECOMENDACIONES:** La Dirección y administración de SUMATEX debe establecer entre sus manuales de funciones y políticas una adecuada segregación de funciones y responsabilidades, adicionando a éstas sanciones por el incumplimiento de las mismas.

11	**OBSERVACIONES:** Existen manuales tanto de funciones, como de procedimientos para el manejo de los sistemas, pero no son de aplicación rigurosa.

Folio 2

Elaborado por:	SCVC
Fecha:	16/02/2014

H.H. 3/5

Folio 1

AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA DE SISTEMAS INFORMÁTICOS

DESARROLLO DE HALLAZGOS

1	**ORGANIZACIÓN AUDITADA:** SUMATEX

2	**PROGRAMA:** Ejecución	**ACTIVIDAD:** Evaluación de actividades de control.

3	**HALLAZGO:** No existen adecuadas medidas de seguridad física de los sistemas informáticos.

4	**CONDICIÓN:** No existen medidas actualizadas de seguridad física de equipos informáticos que contrarresten los riesgos a causa de nuevas amenazas existentes en el entorno.

5	**CRITERIO:** Toda empresa debe contar con medidas de control interno que salvaguarden los recursos de la misma, los que a su vez velen por los intereses de los funcionarios, empleados y clientes, ya que las pérdidas de la empresa también resultan pérdidas para cada uno de los usuarios de la misma.

6	**CAUSA:** La gestión inadecuada informática y el descuido de la administración por prevenir y adoptar medidas de seguridad para los sistemas informáticos.

7	**EFECTO:** La exposición a riesgos que pueden causar pérdidas y daños que pueden llegar a ser irreparables y perjudiciales a los grandes intereses de la empresa**.**

8	**COMENTARIO:** Se debería realizar las evaluaciones necesarias para identificar todos los posibles riegos a los que se puede exponer la empresa y que puedan perjudicar la seguridad de los recursos informáticos y sobre todo de la información contenida en los mismos.

9	**CONCLUSIONES:** La negligencia del supervisor informático de SUMATEX provoca que los recursos informáticos no mantengan la seguridad necesaria para su normal funcionamiento y así brindar confianza a la empresa.

10	**RECOMENDACIONES:** El supervisor informático debe implementar las seguridades físicas necesarias en los sistemas informáticos, para evitar que éstos estén expuestos a riesgos, como: el fraude, robos, uso indebido, desperdicio de tiempo - recursos; y, la extracción de información confidencial, etc.

11	**OBSERVACIONES:** La empresa cuenta con medidas de seguridad básicas que no son suficientes para contrarrestar la cantidad de riesgos existentes.

Folio 2

Elaborado por:	SCVC
Fecha:	16/02/2014

H.H. 4/5

Folio 1

AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA DE SISTEMAS INFORMÁTICOS

DESARROLLO DE HALLAZGOS

1	**ORGANIZACIÓN AUDITADA:** SUMATEX

2	**PROGRAMA:** Ejecución	**ACTIVIDAD:** Evaluación de actividades de control.

3	**HALLAZGO:** No existen medidas de seguridad lógica para los sistemas informáticos.

4	**CONDICIÓN:** No existen medidas de seguridad lógicas en los sistemas informáticos de SUMATEX.

5	**CRITERIO:** La administración debe cumplir con medidas de control interno que salvaguarden los recursos de la empresa, incluidos los recursos del software informático, que aunque para muchos pareciera algo irrelevante, la desatención a este recurso también perjudica el buen desenvolvimiento de las operaciones.

6	**CAUSA:** El descuido y poca atención prestada por parte de los altos directivos de la empresa, ante la aplicación de medidas de seguridad lógica de los sistemas informáticos.

7	**EFECTO:** La exposición de la información, los datos y el manejo de los sistemas ante riesgos desconocidos puede provocar daños irreparables a los intereses de la empresa SUMATEX.

8	**COMENTARIO:** Se deben tener muy en cuenta que los riesgos existentes en el medio ambiente donde se operan los sistemas y software de las empresas, son muy frecuentes y aunque no son identificables a simple vista, se presentan en cualquier negocio y pueden causar serios daños.

9	**CONCLUSIONES:** El Dpto. informático de la Empresa SUMATEX no tiene establecido entre sus objetivos medidas de seguridad lógica; aunque se tomen medidas informales, éstas no son suficientes para contrarrestar la serie de riesgos a los que está expuesta la información sistematizada de la empresa.

10	**RECOMENDACIONES:** El Dpto. Informático debe tomar medidas formales y de evaluación profunda sobre los riesgos a los que se enfrenta la información sistematizada de la empresa, como pueden ser: utilización de firewalls personales, filtrado de paquetes proxy-gateways de aplicaciones, screened subnet, criptología, contraseñas de uso personal, tarjetas de acceso, copias de seguridad, soportes externos, etc.

11	**OBSERVACIONES:** SUMATEX cuenta con medidas básicas de seguridad lógica, pero son manejadas de manera informal; además no posee archivos escritos sobre estas medidas, que por cierto no son suficientes.

Folio 2

Elaborado por:	SCVC
Fecha:	16/02/2014

Folio 1

H.H. 5/5

AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA DE SISTEMAS INFORMÁTICOS

DESARROLLO DE HALLAZGOS

1	**ORGANIZACIÓN AUDITADA:** SUMATEX

2	**PROGRAMA:** Ejecución	**ACTIVIDAD:** Información y comunicación.

3	**HALLAZGO:** Poca fluidez de información e inadecuada comunicación entre los diferentes niveles jerárquicos.

4	**CONDICIÓN:** La escasa fluidez de información y comunicación entre administradores y subordinados.

5	**CRITERIO:** Es necesario mantener la eficiencia en el uso de los sistema de información y comunicación, para que sean éstos los que ayuden a la identificación de necesidades, difusión de requerimientos y a la mejor toma de decisiones.

6	**CAUSA:** Falta de establecimiento de canales formales de comunicación e información que fomenten la confianza y seguridad entre los diferentes niveles jerárquicos de la empresa.

7	**EFECTO:** La poca identificación de necesidades y requerimientos en los diferentes niveles jerárquicos y su correspondiente atención, inadecuado sistema de control interno y el desenvolvimiento informal de actividades del personal de la empresa.

8	**COMENTARIO:** Es necesario mantener un buen sistema de control interno, y para esto es muy importante mantener una adecuada fluidez de información y comunicación que aporte al conocimiento general de las órdenes, controles y funciones que se deben cumplir.

9	**CONCLUSIONES:** Un sistema de información y comunicación poco adecuado hace que no se pueda mantener la confianza necesaria entre los altos funcionarios de la Empresa con sus subordinados, de tal forma que se pueda identificar fácilmente requerimientos y sugerencias de mejoramiento.

10	**RECOMENDACIONES:** La administración de la Empresa SUMATEX debe implementar un sistema de información y comunicación más ágil y moderno que aporte al correcto desarrollo de las funciones, procesos y actividades que se realizan en la empresa, de tal forma que brinde mayor confianza al personal para que puedan emitir sus opiniones y aportes en procura de alcanzar los grandes objetivos empresariales.

11	**OBSERVACIONES:** SUMATEX cuenta con un sistema básico de información y comunicación, que no ha sido manejado de la mejor manera, ni con liderazgo.

Folio 2

Elaborado por:	SCVC
Fecha:	16/02/2014

4.3. COMUNICACIÓN

4.3.1 ACTA DE COMUNICACIÓN DE RESULTADOS.

CONTENIDO DEL BORRADOR DEL INFORME DE AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA DE SISTEMAS INFORMÁTICOS A LA EMPRESA SUMATEX, DE LA CIUDAD DE RIOBAMBA, POR EL PERÍODO 2012.

A los veinte y seis días del mes de Marzo del dos mil catorce, en la ciudad de Riobamba provincia de Chimborazo a las nueve horas, los suscritos: Sra. Sandra Carolina Valdiviezo Crizón en calidad de Auditora y la Ing. Susana Guaraca en calidad de Gerente de SUMATEX, se constituyen en la sala de conferencias de la empresa con el objeto de dejar constancia de la lectura del Borrador del Informe de Auditoría de Seguridad Física y Lógica de los Sistemas Informáticos de la empresa SUMATEX, por el período 2012, examen que fue realizado de conformidad a la propuesta de servicios de auditoría enviada el día tres de Enero del dos mil catorce.

Para el efecto se convocó mediante oficio a los funcionarios principales de la empresa, para que asistan a la presenta diligencia.

Al efecto, en presencia de los altos funcionarios que hacen constar sus firmas más abajo, se procedió a la lectura del borrador del informe, asimismo se analizaron y discutieron los resultados de la Auditoría con sus respectivos: comentarios, conclusiones y recomendaciones descritas en las hojas de hallazgos.

Para constancia de lo discutido, las personas asistentes suscriben la presente acta en dos ejemplares de igual tenor.

Ing. Susana Guaraca Matute	Ing. C.P.A. Paulina Ayala
GERENTE	CONTADORA
C.I.- 060143762-8	C.I.- 060390867-1

Sra. Jenny López
AUXILIAR CONTABLE
CI.-

Ing. Pablo Cruz
SUPERVISOR INFORMÁTICO
CI.-

Ing. Andrés Posada Hernández
CONSULTOR PRODUCTIVO
C.I.-

Sra. Margarita Muñoz
SUPERVISORA DE VENTAS
C.I.-

Sra. María Pilco
JEFE DE BODEGA
C.I.-

Sra. Nancy Saca
JEFE DE PRODUCCIÓN
C.I.-

4.3.2 INFORME FINAL

Riobamba, 27 de Marzo del 2014.

Ingeniera.

Elsa Susana Guaraca Matute

Gerente – Propietaria de SUMATEX

Presente.-

De mi consideración:

A la culminación de la Auditoría de Seguridad Física y Lógica de Sistemas Informáticos aplicada a la empresa SUMATEX de la ciudad de Riobamba, provincia de Chimborazo, por el período 2012, mi responsabilidad es expresar la opinión acerca de los niveles de seguridad física y lógica y el control interno que maneja la empresa, expresados en una opinión clara y concreta del desarrollo de estas medidas de control y si estos se ejecutan de manera idónea con base las Normas de Control Interno.

La Auditoría de Seguridad Física y Lógica de Sistemas Informáticos fue aplicada en base a los componentes del Método COSO II, y Normas de Control Interno establecidos es a la por la Contraloría General del Estado referentes a la tecnología de la información, etc., elementos que nos ha permitido realizar una evaluación objetiva de la situación actual de la empresa e identificar sus falencias y necesidades, que hacen que la seguridad de los recursos informáticos de SUMATEX no sea confiable en su totalidad.

Los componentes analizados dentro de esta Auditoría son: Ambiente Interno, Establecimiento de Objetivos, Identificación de Riesgos, Evaluación de Riesgos, Respuesta al Riesgo, Información, Comunicación y Monitoreo; componentes aplicados a las actividades que se ejercen en la empresa.

En mi opinión, SUMATEX se ajusta a las disposiciones legales vigentes, al dar cumplimiento a las exigencias del Instituto Ecuatoriano de Seguridad Social, Servicio de Rentas Internas y demás entes reguladores a los que está obligada a someterse dicha Empresa; pero a la vez se abstrae de dar cumplimiento a normas de control interno que fomenten el desarrollo de seguridades físicas y lógicas de los sistemas informáticos.

A continuación detallaré los hechos más relevantes encontrados en el proceso de ejecución, evaluación e identificación de riesgos de la Auditoría, los que se resumen de manera puntual en las conclusiones y recomendaciones citadas a continuación:

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIÓN 1.- La gestión informática de la empresa debe ir más allá de identificar los riesgos más frecuentes, es decir brindar seguridad en la manipulación, control y manejo de los equipos informáticos; y, estar en constante monitoreo y evaluación de las necesidades de prevención ante posibles nuevos riesgos.

RECOMENDACIÓN 1.- La administración y gestión del departamento informático deberá adoptar medidas y políticas que salvaguarden los recursos informáticos, tales como: medidas preventivas, medidas de control y medidas correctivas.

CONCLUSIÓN 2.- Es evidente la inexistencia de un adecuado control interno, y la ineficiente segregación de funciones, lo cual provoca la inseguridad en la difusión de la información, el incorrecto uso del sistema y el inadecuado salvaguardo de los recursos.

RECOMENDACIÓN 2: La Dirección y administración de SUMATEX debe establecer en su manual de funciones una adecuada segregación de funciones y responsabilidades para cada puesto de trabajo, adicionando a éste sanciones por el incumplimiento de las mismas.

CONCLUSIÓN 3: La negligencia del supervisor informático de SUMATEX provoca que los recursos informáticos no mantengan la seguridad necesaria para su normal funcionamiento y para brindar confianza a la empresa.

RECOMENDACIÓN 3: El supervisor informático debe implementar las seguridades físicas necesarias en los sistemas informáticos, a fin de evitar que éstos estén expuestos a riesgos

como: el fraude, robos, uso inadecuado, desperdicio de tiempo - recursos; y, la extracción de información confidencial, etc.

CONCLUSIÓN 4: El Dpto. Informático con el que cuenta SUMATEX no tiene establecido entre sus objetivos medidas de seguridad lógica; aunque se han adoptado ciertas medidas informales, que por cierto, no son suficientes para contrarrestar la serie de riesgos a los que está expuesta la información sistematizada de la empresa.

RECOMENDACIÓN 4: El Dpto. Informático debe adoptar medidas formales y de evaluación profunda sobre los riesgos a los que se enfrenta la información sistematizada de la empresa SUMATEX, como pueden ser: firewalls personales, filtrado de paquetes proxy-gateways de aplicaciones, screened subnet, criptología, contraseñas de uso personal, tarjetas de acceso, copias de seguridad, soportes externos, etc.

CONCLUSIÓN 5: Inexistencia de un sistema de información y comunicación adecuado que permita mantener la confianza entre los altos funcionarios de la Empresa con sus subordinados lo que impide identificar requerimientos y sugerencias de mejoramiento.

RECOMENDACIÓN 5: La administración de la Empresa SUMATEX debe implementar un sistema de información y comunicación más ágil y dinámico que aporte al correcto liderazgo y control de las funciones, procesos y actividades que se realizan en la empresa, de tal forma que brinde mayor confianza al personal para que puedan emitir sus opiniones y aportes en procura de una mejor toma de decisiones.

Riobamba, 27 de Marzo del 2014

Sandra Carolina Valdiviezo Crizón
AUDITORA INDEPENDIENTE

CONCLUSIONES

- SUMATEX se ha manejado casi desde sus inicios con una estructura funcional básica sin implementar áreas de control de calidad, control interno y de seguridades informáticas apropiadas, por lo que no se ha podido establecer de manera concreta las necesidades y riesgos a los que se puede enfrentar la empresa en un futuro mediato y a largo plazo.

- SUMATEX no ha sido sometida a Auditoría de Seguridad Física y Lógica de Sistemas Informáticos alguna, por lo que no han podido ser partícipes de la opinión de un profesional que aporte con sus conocimientos para determinar las falencias y carencias reflejadas en esta área; y. sobretodo que les ayude a tener una idea clara de los riesgos a los que se expone la empresa si no se toman medidas para salvaguardar la seguridad de los sistemas informáticos.

- El área informática de SUMATEX no ha considerado la seguridad de los equipos informáticos, por lo que se advierte que el sistema informático utilizado no guarda la seguridad mínima de la información empresarial contenida en éste.

- El desconocimiento, la falta de personal capacitado y el control interno inapropiado a ocasionado que se pase por alto la importancia de la seguridades informáticas, provocando que los empleados de SUMATEX carezcan de una cultura de cuidado y conservación de la información archivada en los sistemas informáticos.

- Finalmente, en SUMATEX no se han aplicado indicadores de gestión, tanto de carácter general, así como de gestión informática, que contribuyan a medir la gestión realizada por el personal de esta organización.

RECOMENDACIONES

- Es necesario implementar medidas de control interno adecuadas a los requerimientos y necesidades de la empresa SUMATEX a fin de brindar seguridad y confianza a los funcionarios y empleados, ya que de su implantación depende el adecuado desarrollo de las actividades de la empresa.

- En los diferentes niveles Jerárquicos que conforman la empresa SUMATEX, es necesario contratar personal con mayor capacidad de dirección y liderazgo que ayude a velar por el cumplimiento de las medidas de control interno, estableciendo nuevos objetivos, actualizando los enunciados de misión y visión, aparte de redefinir las funciones del personal, de tal manera que cada funcionario cumpla a cabalidad con las tareas a ellos encomendadas.

- Es necesario implementar un área de control interno que permita el control y supervisión de los diferentes procesos y funciones del personal, de tal forma que esta unidad pueda adoptar medidas de seguridad físicas y lógicas de los sistemas informáticos y de todos los recursos con los que cuenta la empresa, poniendo especial interés en medidas de: identificación, evaluación, respuesta a riesgos y aplicando medidas de seguridad informática como las antes señaladas en el desarrollo de la auditoría.

- La Dirección de la empresa SUMATEX debe emprender una amplia campaña interna de concienciación y difusión de las medidas de seguridad que son necesarias adoptar para salvaguardar toda la información empresarial automatizada que reposa en los sistemas informáticos existentes, más allá de delimitar funciones y responsabilidades en el manejo de dichos sistemas.

- La administración y dirección de SUMATEX adopte los indicadores aplicados y las medidas de seguridad sugeridas en el transcurso de la auditoría, de tal forma que pueda brindar una confianza relevante en el normal desarrollo de las actividades.

GLOSARIO DE TÉRMINOS

Sistemas de Información (SI): Conjunto de componentes interrelacionados que reúnen, procesan, almacenan y distribuyen datos e información y proporcionan un mecanismo de retroalimentación con el fin de cumplir con un objetivo. (Auditoría Informática Introducción N. CADENA)

Datos: Son hechos aislados, como el número de empleado, el total de horas semanales trabajadas, los números de parte de un inventario o las órdenes de ventas. (A. I. Introducción. N. CADENA)

Información: Conjunto de hechos organizados de tal forma que posee un valor adicional más allá del que tiene cada uno por sí mismo. (A. I. Introducción. N. CADENA)

Proceso: Conjunto de tareas relacionadas de manera lógica que se realizan para llegar a un determinado resultado. (A. I. Introducción. N. CADENA)

Estándar de desempeño del sistema: Objetivo específico del sistema. (A. I. Introducción. N. CADENA)

Pronóstico: Predicción de eventos futuros con el fin de evitar problemas. (A. I. Introducción. N. CADENA)

Sistemas de información basados en computadoras: Conjunto único de hardware, software, bases de datos, telecomunicaciones, personas y procedimientos que se configuran con el fin de recabar, manipular, almacenar y procesar datos para convertirlos en información. (A. I. Introducción. N. CADENA)

Infraestructura tecnológica: Todo el hardware, software, personas y procedimientos que se configuran con el fin de recabar, manipular, almacenar y procesar datos para convertirlos en información. (A. I. Introducción. N. CADENA)

Extranet: Red basada en una tecnología web que permite sólo a algunas personas externas a la organización, como socios de negocios y clientes, el acceso autorizado al recursos de la intranet de la organización. ACHA ITURMENDI, J. José (1994)

Intranet: Red interna basada en tecnología Web que permite al personal de una organización intercambiar información o trabajo de proyectos. ACHA ITURMENDI, J. José (1994)

Procedimiento: Estrategias, políticas, métodos y reglas para utilizar los CBIS. ACHA ITURMENDI, J. José (1994)

Hardware: Equipo de cómputo que se utiliza para llevar a cabo actividades de entrada, proceso, salida y almacenamiento. ECHENIQUE, José A. (2001)

Software: Programas de cómputo de que rigen la operación de un sistema informático. ECHENIQUE, José A. (2001)

Bases de Datos.- Colección de datos pertenecientes a un mismo contexto, organizada de tal modo que el ordenador pueda acceder rápidamente a ella.
Una base de datos relacionar, es aquella en la que las conexiones entre los distintos elementos que forman la base de datos, están almacenadas explícitamente con el fin de ayudar a la manipulación y el acceso a éstos. ECHENIQUE, José A. (2001).

BIBLIOGRAFÍA

- Acha, J. (1994) *Auditoría Informática en la Empresa: Aplicaciones En Producción un Enfoque Operacional.* 1ª ed. Madrid. Editorial Paraninfo.
- Arens, A; Elder, R. y Beasley, M. (2007) *Auditoría: Un enfoque integral,* 11ª ed., México, Pearson Educación.
- Echenique, J. (2001) *Auditoría en Informática.* 2ª ed., México, Mc Graw – Hill Interamericana Editores S.A.
- Cadena N. (2012) *Introducción a los Sistemas informáticos*, Riobamba: ESPOCH. EICA.
- Gómez A. (2013) *Auditoría de seguridad informática* 1ª ed., Bogotá, Ediciones de la U.
- Álvarez G. y Pérez P. (2004) *Seguridad Informática para empresas y particulares.* 1º ed., México. Editorial N/I.
- Hernández, A. (2008) *Informe Diagnóstico y Plan de Acción: Proyecto de Asistencia Técnica Especializada.*, Chimborazo, Capacitación del grupo Asociativo "Coser" de Chimborazo Editorial.
- Hernández, E. (2000) *Auditoría Informática: Un enfoque metodológico y práctico,* 2ª ed., México, Grupo Patria Cultura, S.A. de C.V.
- Piattini M.y Peso E. (2001) *Auditoría Informática: Un enfoque práctico,* 2ª ed., México, Alfaomega Grupo Editor S.A.
- Piattini, M.& Peso, E. (2002 *Control Interno y Auditoría Informática.* 2da ed.,
- Royal P. F (1988) *Seguridad en los Sistemas Informáticos*, México, Ediciones Díaz de Saltos.

LINCOGRAFÍA

- Jaime J. (2010). Auditoría Informática recuperada el 23/12/2013 de: http://www.slideshare.net/jaimedanilosistemas/auditoria-informatica-4835783.
- Julio Ríos recuperado el 5701/2014 de: http://www.monografías.com/trabajos82/la-seguridad-informática/la-seguridad-informática2.shtml#ixzz22qQ9mhsuo
- Luciano Jap. (2012). Seguridad física y lógica. Recuperado el: 15/01/2014 de: http://www.slideshare.net/licianojap/seguridad-fisica-y-logica
- Merlyn Carrasco (2005) San Pedro Sula. Auditoría de sistemas de información. Recuperado el: 21/01/2014 de: http://es.scribd.com/doc/104007826/Auditoria-de-La-Seguridad-Fisica-y-Logica
- Recuperado el: 22/02/2014 de: http://www.pwc.com/d/es/cursos/finanzas-y-analis-cuantitativo/coso-ii-enfoque-para-administración-corporativa-de-riesgos.jhtml
- Recuperado el: 12/03/2014 de: http://www.monografias.com/trabajos14/auditoria/auditoria.shtml#ixzz2qQ74zm68

ANEXOS

ANEXO 1

"Saber para ser"
ESPOCH
ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

CUESTIONARIO DE CONTROL INTERNO

C.C.I. 1/9

Comp. 1

Entidad:	SUMATEX
Área evaluada:	Toda la empresa
Tipo de Auditoría:	Auditoría de Seguridad Física y Lógica de Sistemas Informáticos
Componente:	Ambiente Interno
Alcance:	Conocimiento del ambiente interno de la empresa SUMATEX
Objetivo	Conocer el ambiente con el que se maneja Sumatex

N°	PREGUNTAS	RESPUESTAS SI	NO	N.A.	OBSERVACIONES
1.-	¿Cuenta Sumatex con un código de ética?	28	17		
2.-	¿Los empleados muestran compromiso para con la integridad y valores éticos de la empresa?	34	11		
3.-	¿Se ha establecido y actualizado la misión y visión empresarial?	31	14		
4.-	¿La Dirección de Sumatex está comprometida con el cumplimiento de la misión, visión y objetivos?	26	19		
5.-	¿Sumatex ha establecido un organigrama estructural y funcional?	18	27		
	T O T A L	137	88		

Elaborado por:	Fecha:
SCVC	17/01/2014

"Saber para ser" ESPOCH
ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

CUESTIONARIO DE CONTROL INTERNO

C.C.I. 2/9

Comp. 2

Entidad:	SUMATEX
Área evaluada:	Toda la empresa
Tipo de Auditoría:	Auditoría de Seguridad Física y Lógica de Sistemas Informáticos
Componente:	Establecimiento de Objetivos
Alcance:	Todas las áreas de la empresa
Objetivo	Identificar los objetivos establecidos por la empresa.

N°	PREGUNTAS	RESPUESTAS SI	NO	N.A.	OBSERVACIONES
1.-	¿Se ha planteado objetivos para la Gestión de Tecnologías de la Información?	12	33		
2.-	¿Los objetivos de Sumatex están encaminados al cumplimiento de la misión y visión?	36	9		
3.-	¿Sumatex ha planteado objetivos y responsables para el cumplimiento de cada uno de estos?	38	7		
4.-	¿Entre los objetivos empresariales se ha considerado el cuidado de la seguridad informática?	26	19		
	T O T A L	112	68		

Elaborado por:	Fecha:
SCVC	21/01/2014

CUESTIONARIO DE CONTROL INTERNO

Entidad:	SUMATEX
Área evaluada:	Departamentos Administrativos e informáticos
Tipo de Auditoría:	Auditoría de Seguridad Física y Lógica de Sistemas Informáticos
Componente:	Identificación de Riesgos
Alcance:	Áreas administrativas e Informáticas
Objetivo	Identificar los riesgos existentes en SUMATEX.

N°	PREGUNTAS	RESPUESTAS SI	NO	N.A.	OBSERVACIONES
1.-	¿Se ha realizado un análisis de posibles riesgos en la organización?	7	38		
2.-	¿En la empresa se han contemplado las amenazas ocasionadas por el hombre?	26	19		
3.-	¿Se ha realizado un estudio de los posibles riesgos a los que se puede enfrentar la empresa como incendios, descargas eléctricas, corto circuitos, etc.?	18	27		
4.-	¿Existen problemas informáticos que impidan la correcta realización de las funciones empresariales?	32	13		
5.-	¿La empresa cuenta con medidas de seguridad para los equipos informáticos?	23	22		
	T O T A L	106	119		

Elaborado por:	Fecha:
SCVC	23/01/2014

CUESTIONARIO DE CONTROL INTERNO

Entidad:	SUMATEX
Área evaluada:	Departamentos Administrativos e informáticos
Tipo de Auditoría:	Auditoría de Seguridad Física y Lógica de Sistemas Informáticos
Componente:	Evaluación de riesgos
Alcance:	Áreas administrativas e Informáticas
Objetivo	Medir el grado de seguridad física y lógica que se mantiene en el departamento informático

N°	PREGUNTAS	RESPUESTAS SI	NO	N.A.	OBSERVACIONES
1.-	¿Se han presentado riesgos en la empresa que afecten el cumplimiento de los objetivos organizacionales?	12	3		
2.-	¿Se ha estudiado la posible concurrencia de los riesgos identificados?	4	11		
3.-	¿Ha considerado el grado de perjuicio que pueda ocasionar dichos riesgos?	6	9		
4.-	¿Considera que dichos riesgos pueden perjudicar el cumplimiento de los objetivos empresariales, o que pueda ocasionar consecuencias irreparables?	6	9		
	T O T A L	28	32		

Elaborado por:	Fecha:
SCVC	27/01/2014

Entidad:	SUMATEX
Área evaluada:	Departamentos Administrativos e informáticos
Tipo de Auditoría:	Auditoría de Seguridad Física y Lógica de Sistemas Informáticos
Componente:	Respuesta a los Riesgos
Alcance:	Medidas tomadas por los administrativos
Objetivo	Medir el grado de seguridad física y lógica que se mantiene en el departamento informático

N°	PREGUNTAS	RESPUESTAS SI	NO	N.A.	OBSERVACIONES
1.-	¿Se han considerado medidas de corrección ante posibles daños ocasionados por los riesgos identificados?	10	5		
2.-	¿Se han tomado medidas de precaución para las posibles pérdidas o daños de información?	8	7		
3.-	¿Los sistemas informáticos son considerados como un recurso importante ante la prevención de riesgos?	12	3		
4.-	¿Qué grado de atención se le da a los posibles riesgos identificados por la empresa? ❖ Alto _____ ❖ Medio _____ ❖ Bajo _____				Alta 3 Medio 6 Bajo 6
5.-	¿Se cuenta con planes de contingencias y de manejo de incidencias?	2	13		
	T O T A L	35	40		

Elaborado por:	Fecha:
SCVC	29/01/2014

Entidad:	SUMATEX
Área evaluada:	Departamento Informático
Tipo de Auditoría:	Auditoría de Seguridad Física y Lógica de Sistemas Informáticos
Componente:	Actividades de Control
Alcance:	Seguridades físicas y lógicas
Objetivo	Medir el grado de seguridad física y lógica que se mantiene en el departamento informático

N°	PREGUNTAS	RESPUESTAS SI	NO	N.A.	OBSERVACIONES
1.-	¿Se encuentran claramente definidas las actividades para cumplir con las metas establecidas?	10	5		
2.-	¿Se han establecido actividades para el cuidado de la seguridad informática?	8	7		
	SEGURIDAD FÍSICA				
3.-	¿Existen medidas de seguridad físicas como puertas metálicas ventanas con protección, etc., y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial?	6	9		
4.-	¿SUMATEX cuenta con infraestructura e instalaciones eléctricas seguras y confiables?	11	4		
5.-	¿Se evalúan y controlan permanentemente la seguridad física de las instalaciones informáticas de la empresa?	4	11		
6.-	¿Se controla el acceso de personas ajenas y desautorizadas al departamento informático?	9	6		
7.-	¿Se ha determinado a un responsable para el cuidado físico de los recursos informáticos?	10	5		
8.-	¿Se ha realizado un estudio de las posibles catástrofes como incendios, descargas eléctricas, cortó circuitos, inundaciones, robos, etc. a los que se pueda enfrentar la empresa?	10	5		
9.-	¿Dentro del lugar donde están los equipos existen productos inflamables o que puedan causar daño a las computadoras?	8	7		
10.-	¿Existen cámaras de seguridad, detectores de humo, biométricos, y cualquier otra medida de protección a los departamentos de la empresa?	11	4		
11.-	¿Poseen guardias o alarmas de seguridad en la empresa?	10	5		
12.-	¿Se han instalado equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, supresores pico, UPS, generadores de energía?	12	3		
	T O T A L	109	71		

"Saber para ser" ESPOCH
ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

CUESTIONARIO DE CONTROL INTERNO

C.C.I. 7/9

Comp. 6

N°	PREGUNTAS	RESPUESTAS SI	NO	N.A.	OBSERVACIONES
	SEGURIDAD LÓGICA				
13.-	¿La información susceptible de robo, pérdida o daño se encuentra protegida y resguardada?	11	4		
14.-	¿Cuentan con soportes de datos en un lugar distinto al de los equipos?	6	9		
15.-	¿La empresa tiene implementados firewalls?	11	4		
16.-	¿Existen procedimientos y barreras que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo?	9	6		
17.-	¿Se mantiene programas y procedimientos de detección he inmunización de virus en copias no autorizadas o datos procesados en otros equipos?	11	4		
18.-	¿Los equipos tienen acceso a internet?	14	1		
19.-	¿Tiene algún tipo de restricción para el acceso de páginas web?	2	13		
20.-	¿Poseen claves de bloqueos en los equipos?	3	12		
21.-	¿Puede acceder a los sistemas cualquier persona?	9	6		
22.-	¿Cuentan con manuales para la correcta utilización del sistema?	9	6		
23.-	¿Los programas y sistemas son de utilización exclusiva de un funcionario delegado?	10	5		
24.-	¿El sistema cuenta con claves de acceso para las distintas funciones?	14	1		
25.-	¿En caso de robo de información existen soportes de los datos registrados en los equipos de la empresa?	12	3		
	T O T A L	121	74		

Elaborado por:	Fecha:
SCVC	31/01/2014

"Saber para ser" ESPOCH
ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

C.C.I. 8/9

Comp. 7

CUESTIONARIO DE CONTROL INTERNO

Entidad:	SUMATEX
Área evaluada:	Toda la empresa
Tipo de Auditoría:	Auditoría de Seguridad Física y Lógica de Sistemas Informáticos
Componente:	Información y Comunicación
Alcance:	Todas las áreas de la empresa
Objetivo	Medir el nivel de comunicación existente en SUMATEX

N°	PREGUNTAS	RESPUESTAS SI	NO	N.A.	OBSERVACIONES
1.-	¿Existe un sistema de información?	38	7		
2.-	¿El sistema de información permite conocer si se cumplen los objetivos y metas institucionales con uso eficiente de los recursos?	31	14		
3.-	¿El sistema se información proporciona información confiable para la oportuna toma de decisiones?	6	39		
4.-	¿Se establecen medidas a fin de que la información generada cumpla con las disposiciones legales y administrativas aplicables?	33	12		
5.-	¿Existe una adecuada fluidez de información entre los administrativos y empleados?	17	28		
6.-	¿Las disposiciones, metas y objetivos planteados son comunicados por una vía eficiente y adecuada?	13	32		
7.-	¿Existe y opera un mecanismo para el registro, análisis y atención oportuna y suficiente de quejas o denuncias?	17	28		
	T O T A L	155	160		

Elaborado por:	**Fecha:**
SCVC	03/02/2014

CUESTIONARIO DE CONTROL INTERNO

Entidad:	SUMATEX
Área evaluada:	Toda la empresa
Tipo de Auditoría:	Auditoría de Seguridad Física y Lógica de Sistemas Informáticos
Componente:	Monitoreo
Alcance:	Departamentos Informáticos y Administrativos
Objetivo	Medir el grado de monitoreo que se le da a la empresa

N°	PREGUNTAS	RESPUESTAS SI	NO	N.A.	OBSERVACIONES
1.-	¿Realizan la supervisión permanente y mejora continua de las operaciones y actividades de control?	23	22		
2.-	¿Se realizan procesos de evaluación del desempeño?	29	16		
3.-	¿Se mantiene un registro de las actividades que los Administradores y usuarios realizan sobre un sistema?	8	37		
4.-	¿Existe un registro de las existencias físicas de los recursos?	36	9		
5.-	¿Realizan mantenimientos a los equipos informáticos?	38	7		
6.-	¿Existen procesos de actualización de datos, soportes, archivos y copias?	29	16		
	T O T A L	163	107		

Elaborado por:	Fecha:
SCVC	04/02/2014

ANEXO 2

TCCI

TABULACIÓN DE CUESTIONARIOS DE CONTROL INTERNO BASADOS EN LAS NORMAS COSO II APLICADOS EN LA EMPRESA SUMATEX.

Resultados dados en la evaluación de control interno aplicada a 45 personas divididas de la siguiente manera:
Ambiente Interno, Establecimiento de objetivos, Identificación de riesgos, información y comunicación y monitoreo basadas en las Normas COSO II, de aplicación general a 45 empleados; y para los componentes de evaluación del riesgo, respuesta al riesgo y actividades de control, solamente se aplica al personal administrativo, ventas e informático; dando un total de 15 personas.

COMPONENTE 1: AMBIENTE INTERNO.

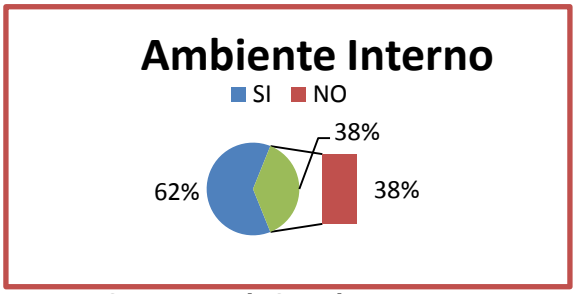
Pregunta 1

¿Cuenta SUMATEX con un código de ética?

SI =	28
NO =	17

Total = 28+17=45

GRÁFICO #1



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

SUMATEX posee un código de ético pero el cual no ha sido actualizado ni puesto a conocimiento del personal de la empresa, por lo que hace que los trabajadores desconozcan las actitudes y valores éticos que tienen que mantener en su lugar de trabajo.

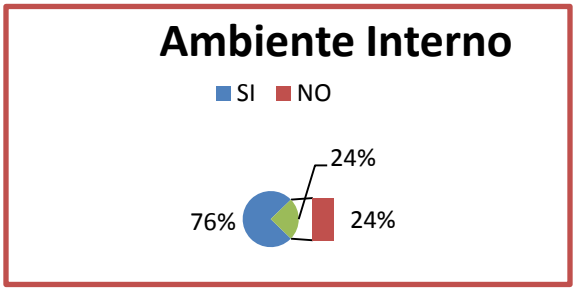
Pregunta 2

¿Los empleados muestran compromiso para con la integridad y valores éticos de la empresa?

SI =	34
NO =	11

Total = 34+11=45

GRÁFICO # 2



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

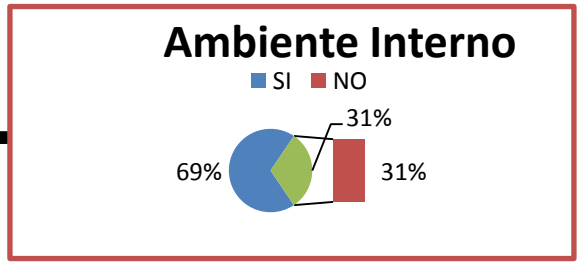
ANÁLISIS

Los empleados si están comprometidos con la empresa aunque desconocen de un código de ética si se ha fomentado valores éticos inculcados día a día con el buen ejemplo de la dirigente que en este caso es la Sra. Gerente.

Pregunta 3

¿Se ha establecido y actualizado la misión y visión empresarial?

GRÁFICO # 3



SI =	31
NO =	14

Total = 31+14=45

Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

SUMATEX ha establecido la misión y visión empresarial, pero no ha sido actualizada por más de 5 años lo que dificulta el desarrollo eficiente y continuo de la empresa pues no se tiene claro de los nuevos retos que se desea alcanzar ni de lo que se ha logrado en el tiempo transcurrido.

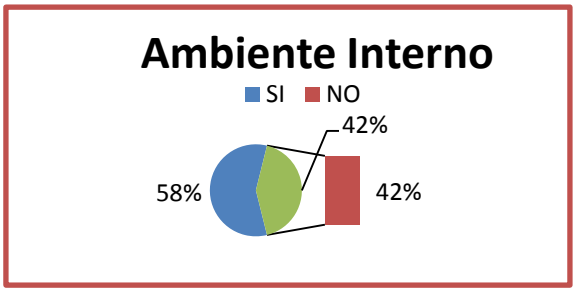
Pregunta 4

¿La Dirección de SUMATEX está comprometida con el cumplimiento de la misión, visión y objetivos?

SI =	26
NO =	19

Total = 26+19=45

GRÁFICO # 4



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

SUMATEX cuenta con una misión y visión empresarial amplia pero éstos no han sido sometidos a un adecuado análisis que determine la eficiencia actual de los mismos; es decir, es necesario identificar si los objetivos han sido ya cumplido o no los motivos por qué, y si estos siguen sirviendo para los próximos años y son de ayuda para el desarrollo empresarial.

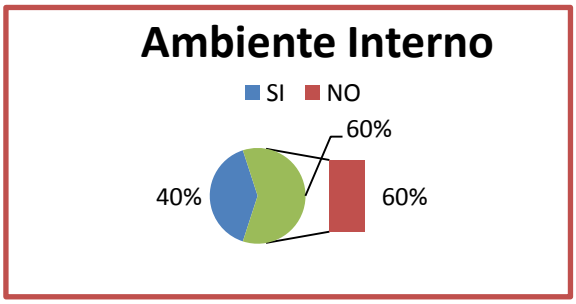
Pregunta 5

¿SUMATEX ha establecido un organigrama estructural y funcional?

SI =	18
NO =	27

Total = 18+27=45

GRÁFICO # 5



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Aunque en este caso muestre la mayoría de respuestas negativas, SUMATEX si cuenta con un organigrama estructural y funcional, pero es de desconocimiento mayoritario lo que implica un desarrollo informal de las actividades.

ANÁLISIS GENERAL DEL COMPONENTE: AMBIENTE INTERNO

SUMATEX muestra un gran nivel de debilidades en cuanto al correcto desarrollo del ambiente interno, ya que no se ha actualizado los objetivos, misión y visión empresarial, no se ha divulgado ni se ha hecho público los valores éticos que se manejan en la misma y todo esto hace que se trabaje de manera informal y sin fundamento sobre las metas que se deben cumplir en un tiempo determinado.

COMPONENTE 2: ESTABLECIMIENTO DE OBJETIVOS

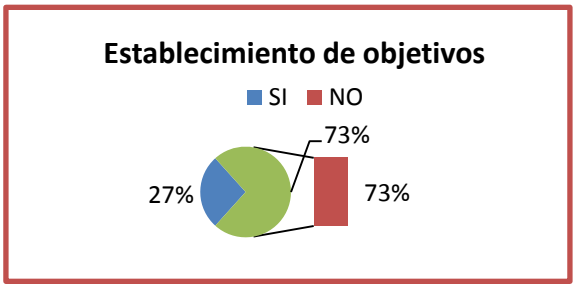
Pregunta 1

¿Se han planteado objetivos para la gestión de Tecnologías de la Información?

SI =	12
NO =	33

Total = 12+33=45

GRÁFICO # 6



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Aunque en la empresa existen planteados objetivos de Gestión empresarial estos son muy poco evaluados, controlados y conocidos por el personal que tiene entre sus funciones el manejo de un equipo informático.

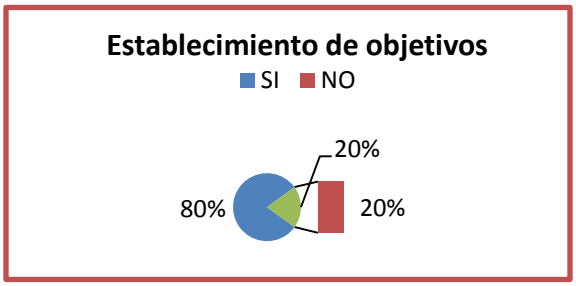
Pregunta 2

¿Los objetivos de SUMATEX están encaminados al cumplimiento de la misión y visión?

SI =	36
NO =	9

Total = 36+9=45

GRÁFICO # 7



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

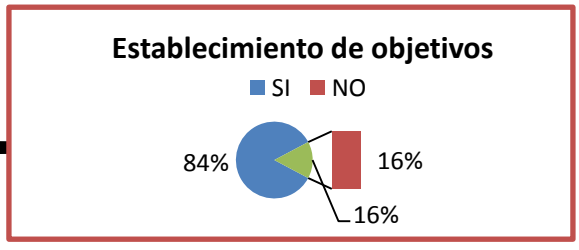
Los objetivos empresariales son los apropiados y encaminados en cuanto al cumplimiento de la misión y visión empresarial; guardando un nivel bajo de desconocimiento por los empleados dados por la falta de comunicación y fluidez de información entre los usuarios internos de SUMATEX.

Pregunta 3

¿SUMATEX ha planteado objetivos y responsables para el cumplimiento de cada uno de estos?

SI =	38

GRÁFICO # 8



NO =	7

Total = 38+7=45

Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

SUMATEX ha establecido la misión y visión empresarial, pero no ha sido actualizada por más de 5 años lo que dificulta el desarrollo eficiente y continuo de la empresa pues no se tiene claro de los nuevos retos que se desea alcanzar ni de lo que se ha logrado en el tiempo transcurrido.

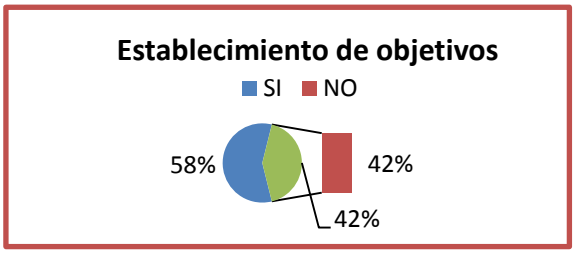
Pregunta 4

¿La Dirección de SUMATEX está comprometida con el cumplimiento de la misión, visión y objetivos?

SI =	26
NO =	19

Total = 26+19=45

GRÁFICO # 9



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

SUMATEX cuenta con una misión y visión empresarial amplia pero éstos no han sido sometidos a un adecuado análisis que determine la eficiencia actual de los mismos; es decir, es necesario identificar si los objetivos han sido ya cumplidos o no, y si estos siguen sirviendo para los próximos años.

ANÁLISIS GENERAL DEL COMPONENTE: ESTABLECIMIENTO DE OBJETIVOS

SUAMTEX ha establecido objetivos pero hace falta la mejora, actualización y distribución adecuada de los objetivos que ayuden y aporten al continuo desarrollo de las actividades empresariales, una vez realizado un análisis de cumplimiento de los objetivos existentes frente a las nuevas metas que se desee alcanzar.

COMPONENTE 3: IDENTIFICACIÓN DE RIESGOS

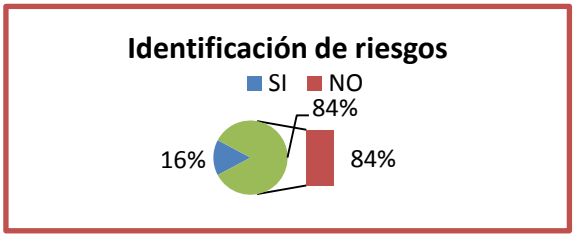
Pregunta 1

¿Se ha realizado un análisis de posibles riesgos en la organización?

SI =	7
NO =	38

Total = 7+38=45

GRÁFICO # 10



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

La administración por sus propios medios y sin hacer uso de la capacidad y apoyo intelectual de los trabajadores ha realizado un análisis de los riesgos que se pueden presentar en la empresa pero no han resultado lo suficientemente eficiente como para contrarrestar los riesgos; las respuestas negativas a esta pregunta es dada por que no se han hecho participes los empleados en este proceso.

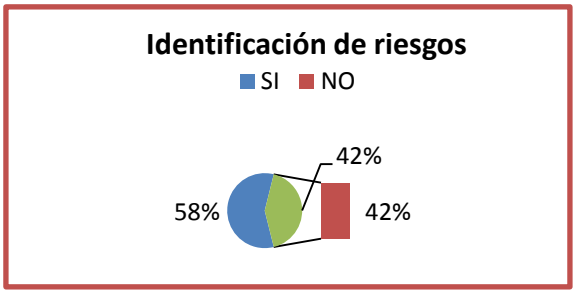
Pregunta 2

¿En la empresa se han contemplado las amenazas ocasionadas por el hombre?

SI =	26
NO =	19

Total = 26+19=45

GRÁFICO # 11



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Se ha contemplado varias amenazas a los que el hombre es el primer causante, como a la vez hay personas que pasan por alto esto, ya sea por desconocimiento o falta de interés dada al cuidado de los recursos de la empresa.

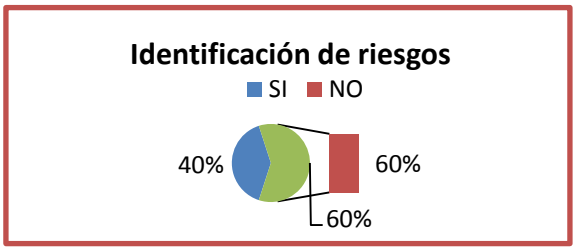
Pregunta 3

¿Se ha realizado un estudio de los posibles riesgos a los que se puede enfrentar la empresa como incendios, descargas eléctricas, corto circuitos, etc.?

SI =	18
NO =	27

Total = 18+27=45

GRÁFICO # 12



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Se denota la falta de interés en realizar un análisis profundo de los posibles daños que pueden ocasionar todos los aspectos antes mencionados, solamente se han tomado medidas de cuidado ante la prevención de descargas eléctricas, pero solo esto no brinda seguridad a la empresa.

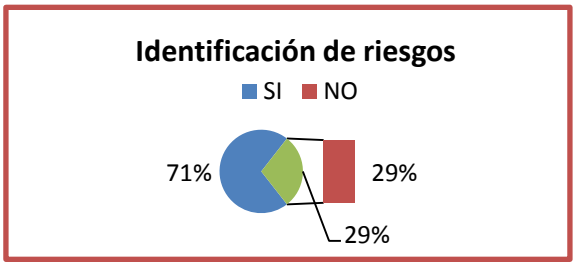
Pregunta 4

¿Existen problemas informáticos que impidan la correcta realización de las funciones empresariales?

SI =	32
NO =	13

Total = 32+13=45

GRÁFICO # 13



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

El acceso a páginas web innecesarias, el acceso al programa contable, archivos, existencias e inventarios a personas que no se les ha autorizado; son unos de tantos problemas que perjudican el correcto desarrollo de las actividades empresariales dentro de los sistemas informáticos.

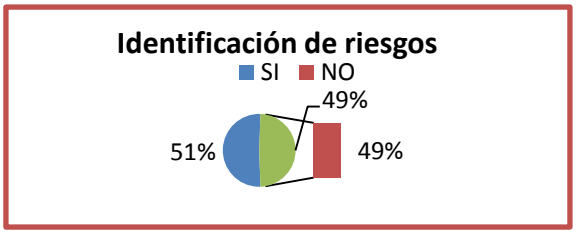
Pregunta 5

GRÁFICO # 14

¿La empresa cuenta con medidas de seguridad para los equipos informáticos?

SI =	23
NO =	22

Total = 23+22=45



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Sin dejar de considerar que si se han tomado medidas de seguridad para el manejo y cuidado de los sistemas informáticos podemos denotar que las medidas tomadas hasta el momento no son de conocimiento general para todos los trabajadores y aún más importante por los que tienen a su cargo la responsabilidad de un equipo; pero aún peor a esto es que no se han tomado las medidas suficientes para brindar confianza a los mismos.

ANÁLISIS GENERAL DEL COMPONENTE: IDENTIFICACIÓN DE RIESGOS.

Se ha considerado en este componente que se debe tomar medidas para mejorar el método o sistema de identificación de riesgos, ya que no existe las medidas suficiente para identificar los verdaderos riesgos sean estos relevantes o no ante el cuidado de los recursos de la empresa y más aún de los recursos informáticos ya que de estos depende mucho el desarrollo y cumplimiento de los objetivos empresariales de SUMATEX.

COMPONENTE 4: EVALUACIÓN DE RIESGOS.

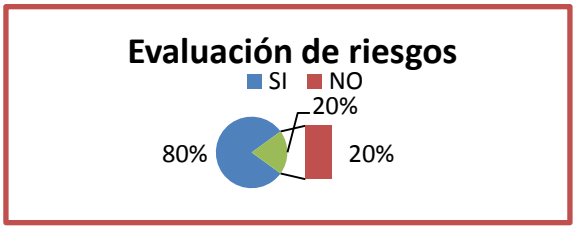
Pregunta 1

¿Se han presentado riesgos en la empresa que afecten el cumplimiento de los objetivos organizacionales?

SI =	12
NO =	3

Total = 12+3=15

GRÁFICO # 15



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

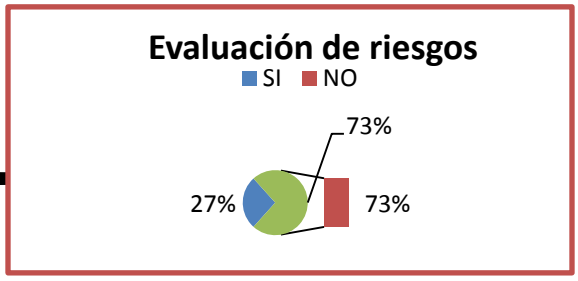
Son muchos de los riesgos que se pueden hablar en este punto y los que pueden afectar seriamente al cumplimiento de los objetivos de SUMATEX, como son la pérdida de información, el robo y daño de información importante, los incendios, y muchos riesgos a los que no han sido aún identificados por la empresa y mucho menos tomado medidas de prevención.

Pregunta 2

¿Se ha estudiado la posible concurrencia de los riesgos identificados?

SI =	4

GRÁFICO #16



NO =	11

Total = 4+11=15

Fuente: Cuestionarios de Control Interno

Realizado por: SCVC

ANÁLISIS

Si ha mostrado muy poco interés en la identificación de los riesgos aún peor se ha estudiado la concurrencia con que se puedan enfrentar los mismos, aunque no se puede dejar pasar que si se han realizado estudios del desempeño de maquinarias y velocidad de equipos informáticos por lo que se pueden tomar como medidas de identificación de concurrencia de riesgos.

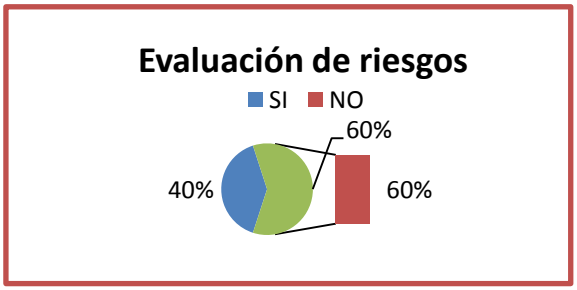
Pregunta 3

¿Ha considerado el grado de perjuicio que puede ocasionar dichos riesgos?

SI =	6
NO =	9

Total = 6+9=15

GRÁFICO # 17



Fuente: Cuestionarios de Control Interno

Realizado por: SCVC

ANÁLISIS

La mayoría no tiene una idea clara de los perjuicios que pueden ocasionar los riesgos en la empresa, por tanto casi no se han tomado precauciones ni se ha aportado de manera intelectual en la mejor toma de decisiones.

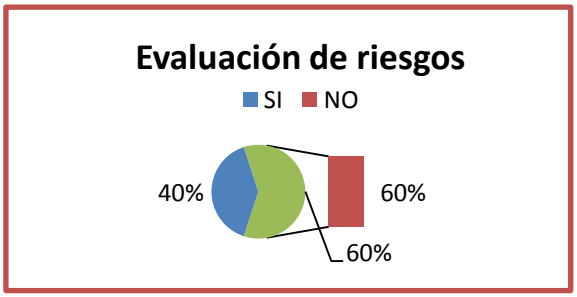
Pregunta 4

¿Considera que dichos riesgos puedan perjudicar el cumplimiento de los objetivos empresariales, o que pueda ocasionar consecuencias irreparables?

SI =	6
NO =	9

Total = 6+9=15

GRÁFICO # 18



Fuente: Cuestionarios de Control Interno

Realizado por: SCVC

ANÁLISIS

Si hay una consideración razonable sobre lo que estos riesgos puedan ocasionar, pero no se ha creado conciencia en todos o casi todos los usuarios internos sobre el grado de afectación al que se puede enfrentar Sumatex.

ANÁLISIS GENERAL DEL COMPONENTE: EVALUACIÓN DE RIESGOS.

Hay mucho porque hacer para la mejora de la evaluación de los riesgos en Sumatex, pues se han mostrado muchas falencias en cuanto a medir el grado de perjuicio de los riesgos, los daños que pueden ocasionar, y la concurrencia con los que se puedan presentar., y esto hace necesaria la aplicación de métodos de evaluación para brindar opiniones para la mejor toma de decisiones.

COMPONENTE 5: RESPUESTA AL RIESGO.

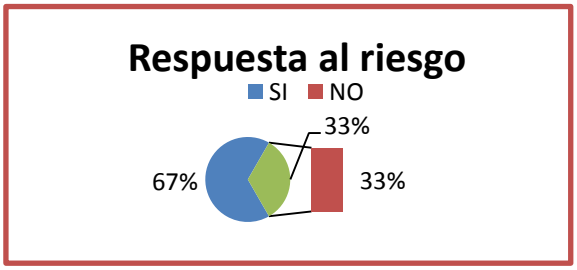
Pregunta 1

¿Se han considerado medidas de corrección ante posibles daños ocasionados por los riesgos identificados?

SI =	10
NO =	5

Total = 10+5=15

GRÁFICO # 19



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Si se han tomado las medidas de corrección correspondientes a los riesgos que han sido identificados pero estos son muy pocos frente a la cantidad de riesgos que existen en el medio.

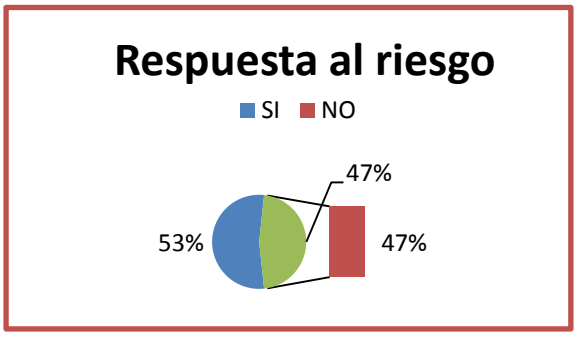
Pregunta 2

¿Se han tomado medidas de precaución para las posibles pérdidas o daños de información?

SI =	8
NO =	7

Total = 8+7=45

GRÁFICO # 20



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Las medidas que se han tomado si contrarrestan los riesgos más relevantes que pueden existir en las empresas pero aún faltan muchas medidas que se deben tomar para estar preparados para enfrentar la variedad de riesgos que existen en el medio.

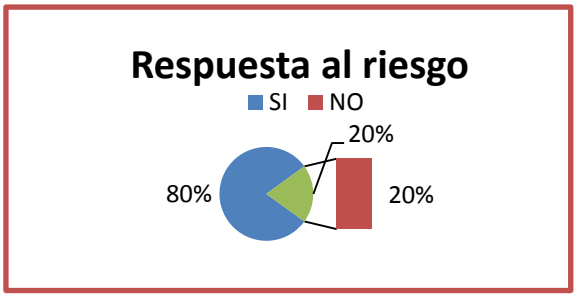
Pregunta 3

GRÁFICO # 21

¿Los sistemas informáticos son considerados como un recurso importante ante la prevención de riesgos?

SI =	12
NO =	3

Total = 12+3=15



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

La mayoría sabe claramente que los recursos informáticos resultan bastante importantes ante la prevención de riesgos, incluso los demás recursos son muy importantes, pero la atención que se les da resulta escasa.

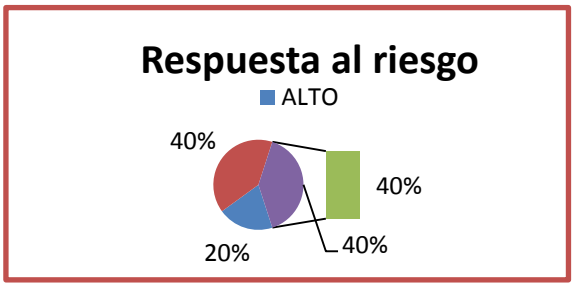
Pregunta 4

¿Qué grado de atención se le da a los posibles riesgos identificados por la empresa?

ALTA =	3
MEDIO =	6
BAJO =	6

Total = 3+6+6=15

GRÁFICO # 22



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Las atenciones dadas a los riesgos identificados por la empresa son bajos cuando deberían ser altos y atendidos de manera eficiente, para poder mantener un nivel de confianza alto en el continuo desarrollo de las actividades.

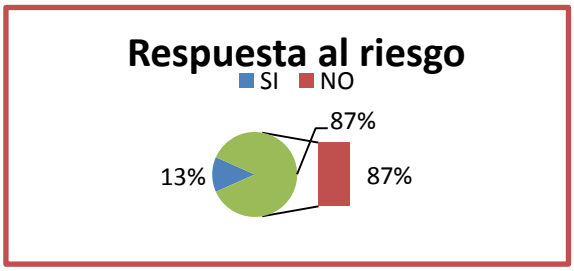
Pregunta 5

¿Se cuenta con planes de contingencia y de manejo de incidencias?

SI =	2
NO =	13

Total = 2+13=15

GRÁFICO # 23



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

No mantienen un archivo formal de planes de contingencia y de manejo de incidencias, por lo mismo hace que el personal desconozca los mismos, solo se ha difundido de manera verbal ante ciertas personas los posibles planes de contingencias que se puedan aplicar en la empresa.

ANÁLISIS GENERAL DEL COMPONENTE: RESPUESTA AL RIESGO.

SUMATEX si ha dado respuesta a los pocos riesgos que ha identificado, pero le falta mucho que identificar y aún más dar respuesta a los mismos, para continuar con normal desarrollo de las operaciones y actividades a las que se dedica la empresa.

COMPONENTE 6: ACTIVIDADES DE CONTROL.

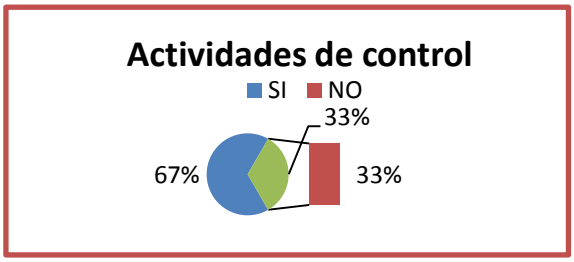
Pregunta 1

¿Se encuentra claramente definidas las actividades para cumplir con las metas establecidas?

SI =	10
NO =	5

Total = 10+5=15

GRÁFICO # 24



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Si tienen definidas las funciones que deben realizar para cumplir los objetivos primordiales en la empresa pero faltan mucho más funciones por definir para cumplir de manera total y completa las metas de SUMATEX.

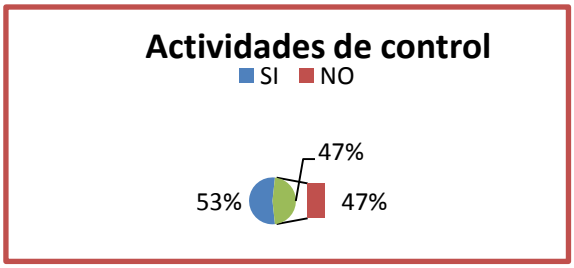
Pregunta 2

¿Se han establecido actividades para el cuidado de la seguridad informática?

SI =	8
NO =	7

Total = 8+7=15

GRÁFICO # 25



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Si se han establecido actividades para el cuidado de la seguridad informática pero aún hacen falta muchos puntos que atender y falencias que corregir en cuanto a actividades que protejan los equipos informáticos tanto de manera física como lógica.

SEGURIDAD FÍSICA

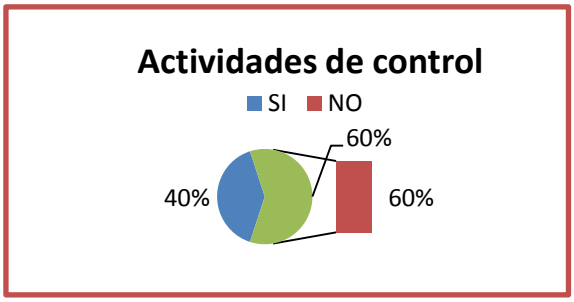
Pregunta 3

¿Existen medidas de seguridad físicas como puertas metálicas, ventanas con protección, etc., y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial?

SI =	6
NO =	9

Total = 6+9=15

GRÁFICO # 26



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Existen muy pocas protecciones y medidas de seguridad para el cuidado de los recursos, pues solamente existen como alarmas, ventanas metálicas y cámaras de seguridad, pero cámaras de humo, cámaras en áreas primordiales como bodega, gerencia, departamento informático, medidas de seguridad industrial son casi nulas.

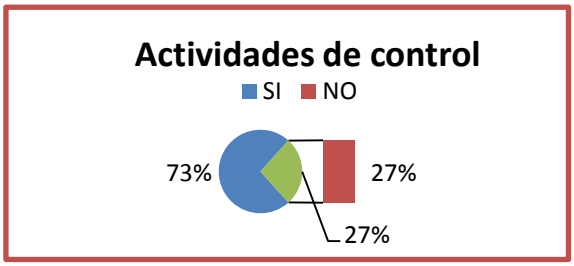
Pregunta 4

¿Sumatex cuenta con infraestructura e instalaciones eléctricas seguras y confiables?

SI =	11
NO =	4

Total = 11+4=15

GRÁFICO # 27



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

La infraestructura con la que cuenta Sumatex es buena y resulta confiable y en cuanto a las instalaciones eléctricas también son casi seguras en su totalidad, aunque siempre hay una posibilidad de fallas ante cortos circuitos y descargas eléctricas.

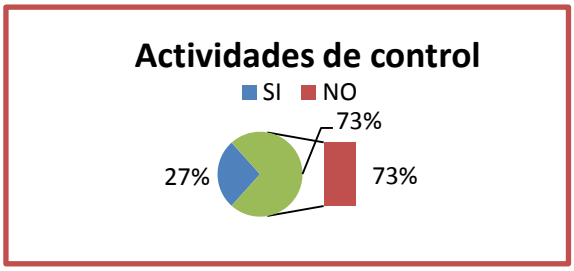
Pregunta 5

¿Se evalúan y controlan permanentemente la seguridad física de las instalaciones informáticas de la empresa?

SI =	4
NO =	11

Total = 4+11=15

GRÁFICO # 28



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Casi no se realizan actividades de control de manera permanente para el cuidado de la seguridad física por lo que hace que la seguridad de los sistemas informáticos sea muy poco confiable.

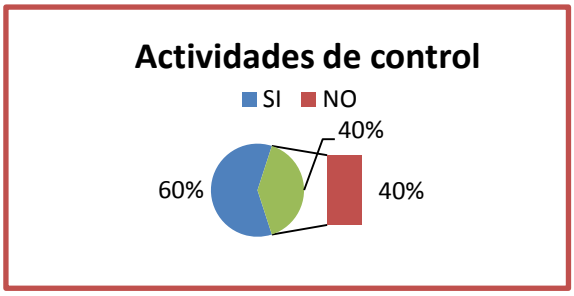
Pregunta 6

GRÁFICO # 29

¿Se controla el acceso de personas ajenas y desautorizadas al departamento informático?

SI =	9
NO =	6

Total = 9+6=15



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

El acceso del personal al departamento informático si es controlado pero no en su totalidad ni de manera tan formal ya que por confianzas dadas se falta a este mandado, y hace que se provoque poca seguridad en el departamento.

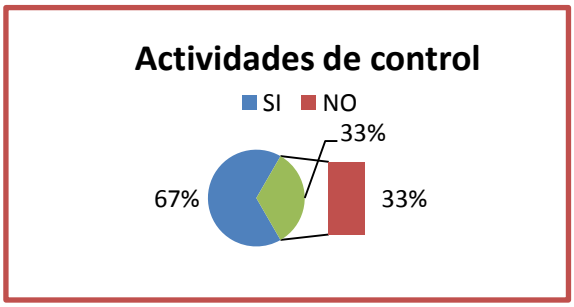
Pregunta 7

GRÁFICO # 30

¿Se ha determinado a un responsable para el cuidado físico de los recursos informáticos?

SI =	10
NO =	5

Total = 10+5=15



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Si tienen determinado un responsable para el cuidado de los equipos informáticos pero para provocar su deficiencia este responsable es el mismo encargado de todos los equipos lo que le hace una responsabilidad muy grande y por ende la inadecuada realización de sus funciones.

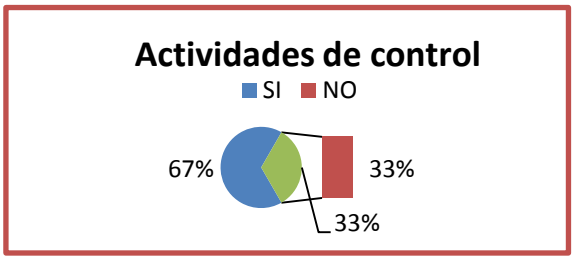
Pregunta 8

GRÁFICO # 31

¿Se ha realizado un estudio de las posibles catástrofes como incendios, descargas eléctricas, corto circuitos, inundaciones, robos, etc., a los que puede enfrentar la empresa?

SI =	10
NO =	5

Total = 10+5=15



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

El estudio sobre los riesgos más relevantes a los que se puede enfrentar la empresa se ha hecho, pero medidas para prevenir perdidas severas o para contrarrestar los mismos aún no se han considerado.

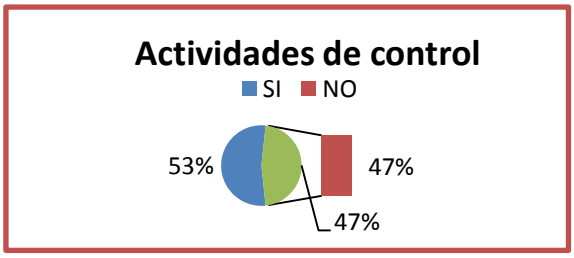
Pregunta 9

GRÁFICO # 32

¿Dentro del lugar donde están los equipos, existen productos inflamables o que puedan causar daños a las computadoras?

SI =	8
NO =	7

Total = 8+7=15



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

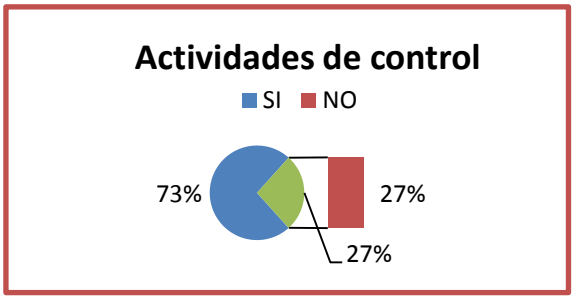
La presencia de telas y pelusas hace que sea inflamable ya que se puede producir un incendio con una mínima chispa, aunque a la vez no se han detentado líquidos inflamables o peligrosos.

Pregunta 10 **GRÁFICO # 33**

¿Existen cámaras de seguridad, detectores de humo, biométricos y cualquier otra medida de control y protección en la empresa?

SI =	11
NO =	4

Total = 11+4=15



Fuente: Cuestionarios de Control Interno
Realizado por: Carolina Valdiviezo

ANÁLISIS

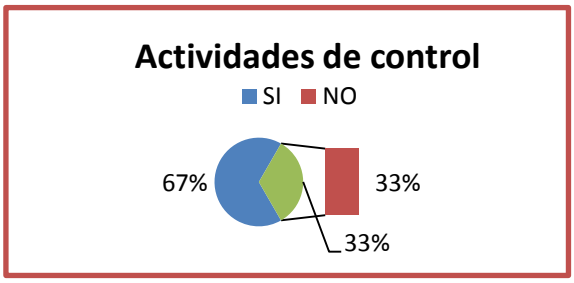
Sumatex cuenta con cámaras de seguridad pero no en todos sus departamentos, no posee cámaras de humo ni biométricos, solo medidas de control de asistencia remotas a cargo de una responsable por área y seguridades físicas básicas.

Pregunta 11 **GRÁFICO # 34**

¿Posee guardias o alarmas de seguridad en la empresa?

SI =	10
NO =	5

Total = 10+5=15



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

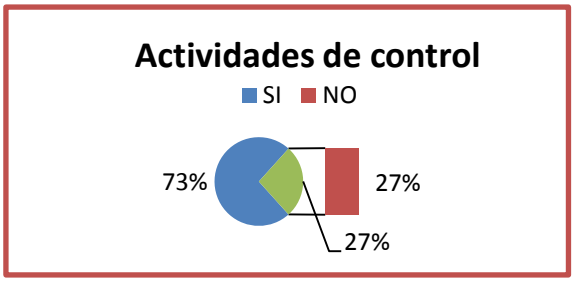
Existen alarmas de seguridad pero no cuentan con guardias de seguridad dada por la extensión y tamaño de la empresa que en este caso resulta casi innecesaria.

Pregunta 12 **GRÁFICO # 35**

¿Se han instalado equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de energía, supresores pico, UPS, y generadores de energía?

SI =	12
NO =	3

Total = 11+4=15



Fuente: Cuestionarios de Control Interno
Realizado por: Carolina Valdiviezo

ANÁLISIS

La mayoría de medidas de seguridad y control antes mencionadas si cuenta la empresa a excepción de generadores de energía a la que pueden recurrir en caso de un corte de energía y UPS.

SEGURIDAD LÓGICA

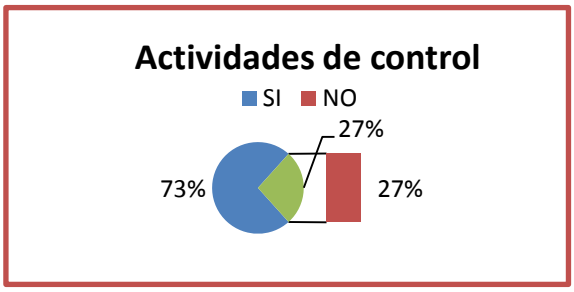
Pregunta 13

GRÁFICO # 36

¿La información susceptible de robo, pérdida o daño se encuentra protegida y resguardada?

SI =	11
NO =	4

Total = 11+4=15



Fuente: Cuestionarios de Control Interno
Realizado por: Carolina Valdiviezo

ANÁLISIS

La empresa si mantiene soportes externos de información en caso de pérdidas y claves de seguridad para el acceso de cierta información para evitar robos, más aún carece de seguridades más fuertes para la protección ante virus, hackers y ladrones de la web.

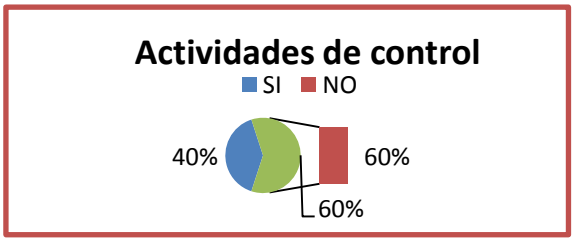
Pregunta 14

GRÁFICO # 37

¿Cuentan con soportes de datos en un lugar distinto al de los equipos?

SI =	6
NO =	9

Total = 6+9=15



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

La información generada en la empresa si es mantenida en soportes pero no de manera externa ni la actualización de estos es tan a menuda como debería.

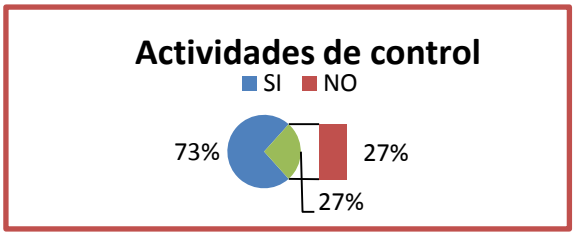
Pregunta 15

GRÁFICO # 38

¿La empresa tiene implementados firewall?

SI =	11
NO =	4

Total = 11+4=15



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

La protección a través de firewall es parte de la seguridad que mantiene la empresa, pero estos no son suficientes para enfrentar todos los riesgos lógicos existentes.

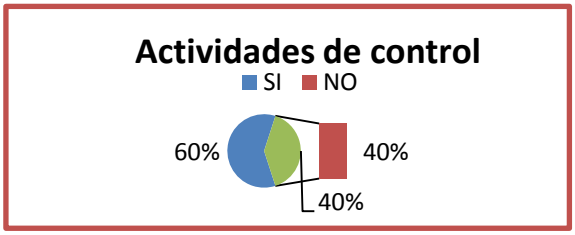
Pregunta 16

GRÁFICO # 39

¿Existen procedimientos y barreras que resguarden el acceso a los datos y sólo se permita acceder a ellos las personas autorizadas para hacerlo?

SI =	9
NO =	6

Total = 9+6=15



Fuente: Cuestionarios de Control Interno
Realizado por: Carolina Valdiviezo

ANÁLISIS

Sumatex y su sistema informático contable mantiene medidas de seguridad para el acceso de personas no autorizadas, pero estas medidas no son cumplidas a cabalidad ni respetadas al 100%.

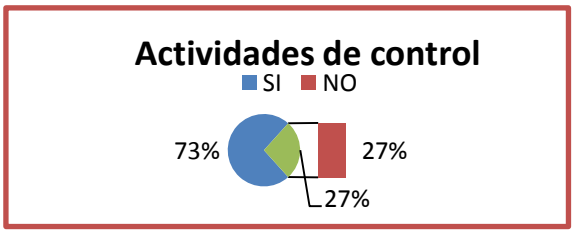
Pregunta 17

GRÁFICO # 40

¿Se mantiene programas y procedimiento de detección he inmunización de virus en copias no autorizadas o datos procesados en otros equipos?

SI =	11
NO =	4

Total = 11+4=15



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

El departamento informático mantiene barreras de protección ante inmunizaciones de virus para los datos procesados por otros equipos, pero no hay un buen control en cuanto a las copias no autorizadas.

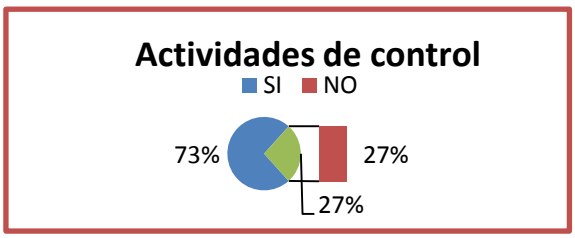
Pregunta 18

GRÁFICO # 41

¿Los equipos tienen acceso a internet?

SI =	14
NO =	1

Total = 14+1=15



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Todos los equipos tienen acceso a internet por ser necesario a excepción de una que se encuentra en bodega la que no necesariamente tiene que estar conectada a internet.

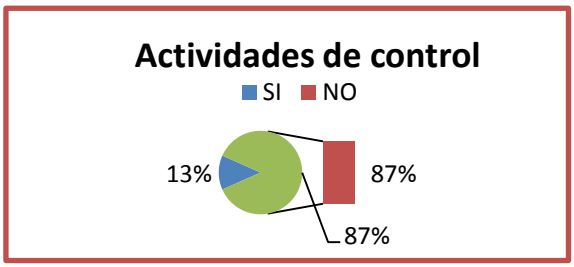
Pregunta 19

¿Tiene algún tipo de restricción para el acceso de páginas web?

SI =	2
NO =	13

Total = 2+13=15

GRÁFICO # 42



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

El acceso a páginas web innecesarias es frecuente ya que no existe un control adecuado lo que puede provocar el mal uso de los recursos de la empresa y más aún la pérdida de tiempo, que conlleva al lento desenvolvimiento de las funciones y la falta de interés de los funcionarios.

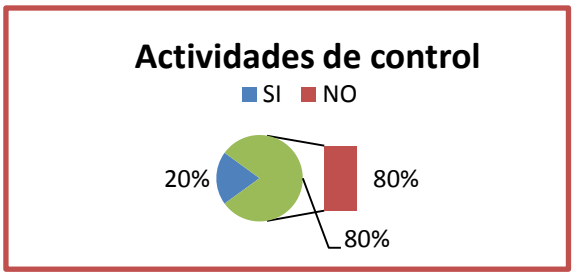
Pregunta 20

¿Posee claves de bloqueos en los equipos?

SI =	3
NO =	12

Total = 3+12=15

GRÁFICO # 43



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Los equipos no poseen claves solo existen claves en el acceso del programa informático contable para ciertas funciones pero mas no para los equipos, y las claves existentes no son respetadas ni de confidencialidad total.

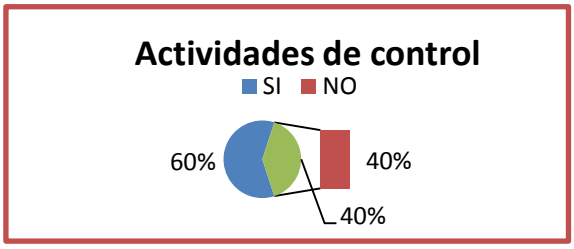
Pregunta 21

¿Puede acceder a los sistemas cualquier persona?

SI =	9
NO =	6

Total = 9+6=15

GRÁFICO # 44



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Los personas tienen acceso a los equipos sin distinción de las funciones que deben cumplir y si de estos están autorizados o no para su acceso.

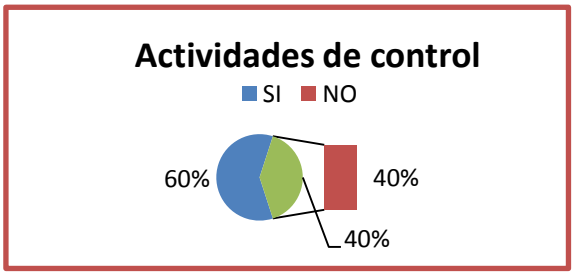
Pregunta 22

¿Cuentan con manuales para la correcta utilización del sistema?

SI =	9
NO =	6

Total = 9+6=15

GRÁFICO # 45



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Existen manuales de manejo y funcionamiento de los sistemas informáticos pero estos no han sido difundidos ni puestos a disposición de todos aquellos empleados que tienen a su cargo el uso de un equipo informáticos por lo que hace que desconozcan el mismo.

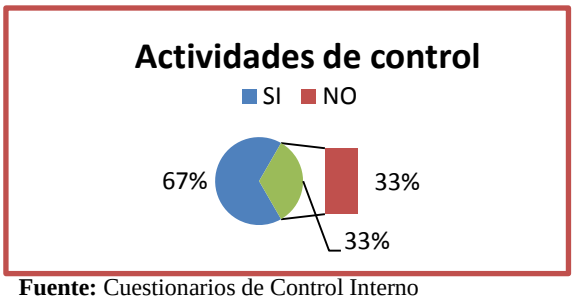
Pregunta 23

¿Los programas y sistemas son de utilización exclusiva de un funcionario delegado?

SI =	10
NO =	5

Total = 10+5=15

GRÁFICO # 46



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Las funciones están dirigidas y delegadas a un funcionario en específico, pero en caso de ausencia se le es otorgada a cualquier otra persona sin posteriormente hacer los respectivos cambios de claves para mantener la seguridad en el acceso del sistema.

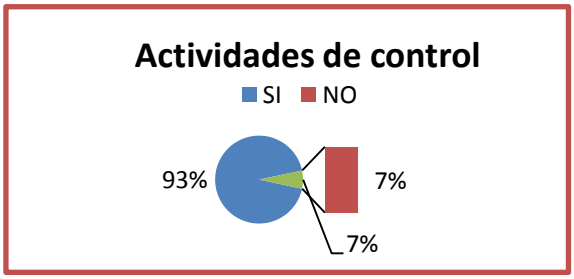
Pregunta 24

¿El sistema cuenta con claves de acceso para las distintas funciones?

SI =	14
NO =	1

Total = 14+1=15

GRÁFICO # 47



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Cada función del sistema cuenta con claves de acceso para personas delegadas para el cargo.

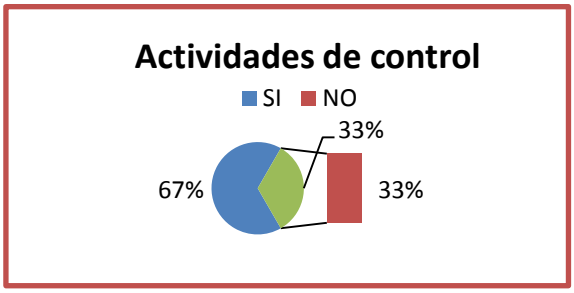
Pregunta 25

¿En caso de robo de información existen soportes de los datos registrados en los equipos de la empresa?

SI =	12
NO =	3

Total = 12+3=15

GRÁFICO # 48



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Existen soportes en memorias externas de todos los datos de la empresa pero no son mantenidos en otro lugar distintos a la empresa.

ANÁLISIS GENERAL DEL COMPONENTE: ACTIVIDADES DE CONTROL.

Las actividades de control existentes si ha ayudado a la mejora del sistema pero hace falta mejorar aún más para que continúe en desarrollo la empresa, ya que es de suma importancia implementar actividades que aporten al control y buen desarrollo de las funciones.

COMPONENTE 7: INFORMACIÓN Y COMUNICACIÓN

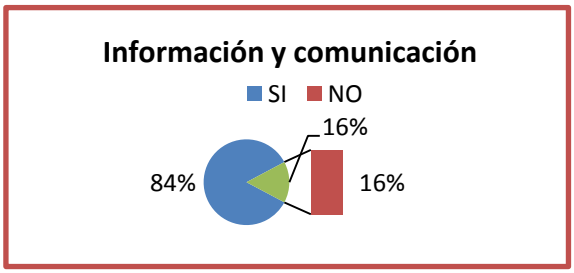
Pregunta 1

¿Existe un sistema de información y comunicación?

SI =	38
NO =	7

Total = 38+7=45

GRÁFICO # 49



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

El manejo de la información es manejada casi confidencialmente, no existe una adecuada fluidez de información, ni métodos de comunicación ante todo el personal que trabaja en la empresa.

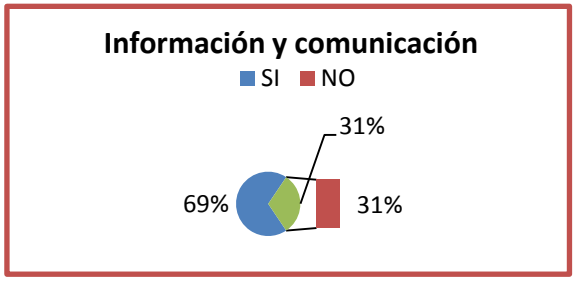
Pregunta 2

¿El sistema de información permite conocer si cumplen los objetivos y metas institucionales con el uso eficiente de los recursos?

SI =	31
NO =	14

Total = 31+14=45

GRÁFICO # 50



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Al no existir una buena comunicación provoca que el personal no sepa con claridad si se van o no cumpliendo con las metas institucionales.

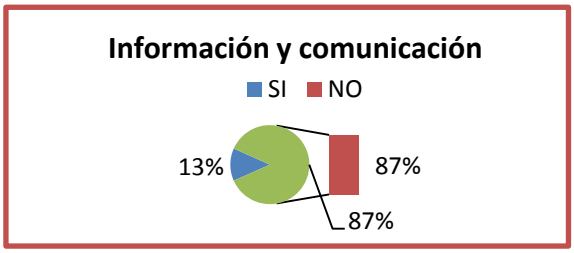
Pregunta 3

¿El sistema de información proporciona información confiable para la oportuna toma de decisiones?

SI =	6
NO =	39

Total = 6+39=45

GRÁFICO # 51



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Si no existe una buena fluidez de información no podrá aportar para la toma de decisiones aún que esta resulte confiable o no.

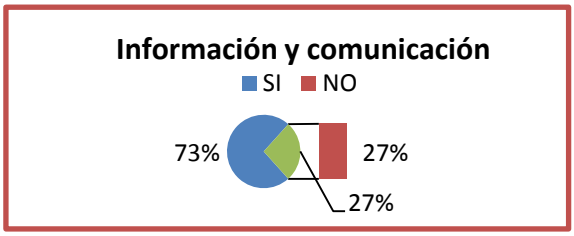
Pregunta 4

¿Se establecen medidas a fin de que la información generada cumpla con las disposiciones legales y administrativas aplicables?

SI =	33
NO =	12

Total = 33+12=45

GRÁFICO # 52



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Existen políticas, normas y medidas de control en cuanto a la expansión y control de la información para que esta vaya acorde a los que establece la ley y a lo que requiere la administración.

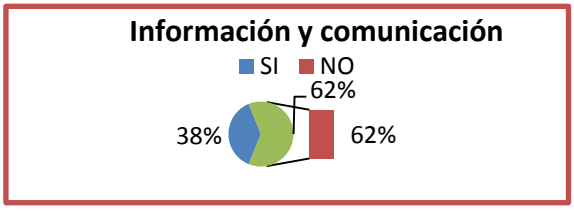
Pregunta 5

¿Existe una adecuada fluidez de información entre los administrativos y empleados?

SI =	17
NO =	28

Total = 17+28=45

GRÁFICO # 53



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

El grado de confianza y libertad de expresión existente en la empresa es poco amplia ya que no hay una libre fluidez de opiniones entre los empleados y la administración que en este caso sería la gerente, dando como resultado la desconfianza y falta de liderazgo.

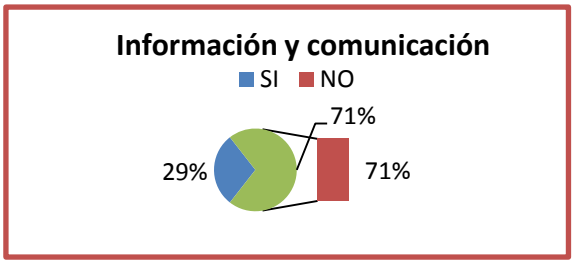
Pregunta 6

GRÁFICO # 54

¿Las disposiciones, metas y objetivos planteados son comunicados por una vía eficiente y adecuada?

SI =	13
NO =	32

Total = 13+32=45



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Los objetivos, metas y disposiciones si mantienen una vía adecuada de comunicación pero no hace uso de los mismos para la distribución equitativa y general de la información.

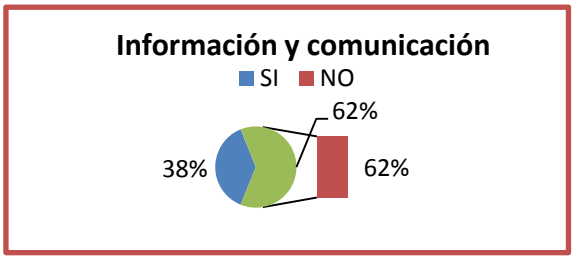
Pregunta 7

GRÁFICO # 55

¿Existe y opera un mecanismo para el registro, análisis y atención oportuna y suficiente de quejas o denuncias?

SI =	17
NO =	28

Total = 17+28=45



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

No existe un método ni mecanismo de atención de quejas o denuncias de los usuarios internos y externos de Sumatex por lo que no se puede identificar el grado de conformidad y satisfacción de los servicios dados por la empresa.

ANÁLISIS GENERAL DEL COMPONENTE: INFORMACIÓN Y COMUNICACIÓN

Es necesario realizar un análisis de las debilidades y falencias que tienen los métodos de información y comunicación de Sumatex, para así brindar una opinión adecuada para la mejora y toma de decisiones correctas, con los que se espera mejorar el liderazgo de los administrativos, el desempeño de los empleados y la conformidad de los usuarios externos.

COMPONENTE 8: MONITOREO

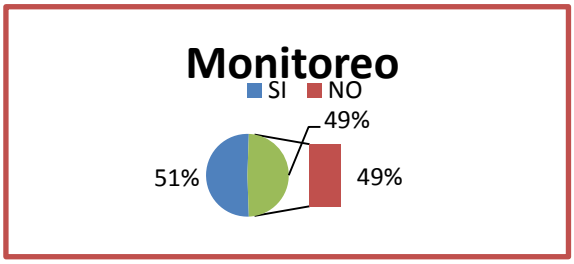
Pregunta 1

GRÁFICO # 56

¿Realizan la supervisión permanente y mejora continua de las operaciones y actividades de control?

SI =	23
NO =	22

Total = 23+22=45



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Si hay la supervisión permanente en los procesos de operación pero aún falta la mejora continua de las actividades de control, para hacer de estos procesos los adecuados.

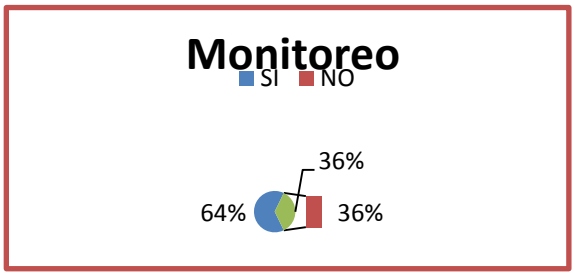
Pregunta 2

¿Se realizan procesos de evaluación del desempeño?

SI =	29
NO =	16

Total = 29+16=45

GRÁFICO # 57



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Existen controles y evaluaciones del desempeño del personal del departamento de producción, mas no de los demás departamentos a los cuales si se deberían considerar para este proceso.

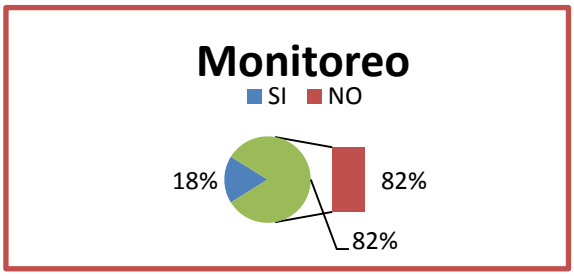
Pregunta 3

¿Se mantiene un registro de las actividades que los administradores y usuarios realizan sobre el sistema?

SI =	8
NO =	37

Total = 8+37=45

GRÁFICO # 58



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Solo se puede determinar las actividades que realiza cada uno de los usuarios a través de la información que contiene cada equipo, mas no se cuenta con un registro adecuado de los mismos.

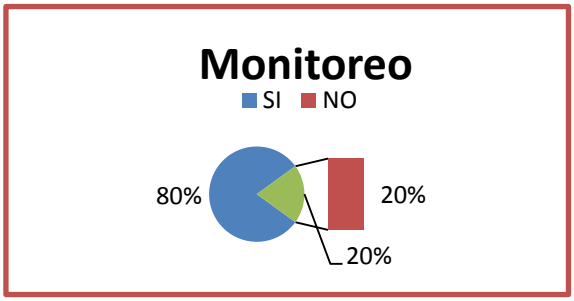
Pregunta 4

¿Existe un registro de las existencias físicas de los recursos?

SI =	36
NO =	9

Total = 36+9=45

GRÁFICO # 59



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Sumatex maneja un sistema de inventarios pero es aplicada, pero no se realiza un control permanente ni es controlado regularmente el mismo por lo que hace que existe dicho registro.

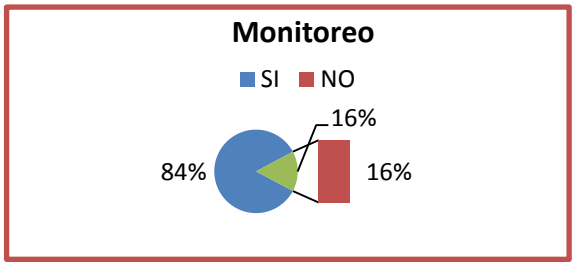
Pregunta 5

GRÁFICO # 60

¿Realizan mantenimientos a los equipos informáticos?

SI =	38
NO =	7

Total = 38+7=45



Fuente: Cuestionarios de Control Interno
Realizado por: SCVC

ANÁLISIS

Los equipos son sometidos a mantenimientos y controles de funcionamiento tanto en el sistema informático contable como en el soporte técnico de todo el equipo.

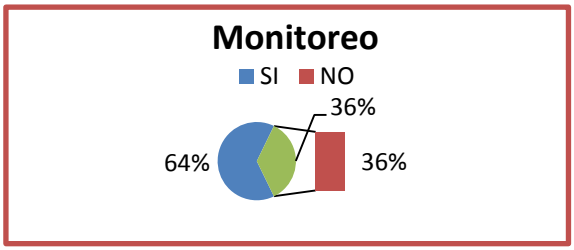
Pregunta 6

¿Existen procesos de actualización de datos, soportes, archivos y copias?

SI =	29
NO =	16

Total = 29+16=45

GRÁFICO # 61



Fuente: Cuestionarios de Control Interno
Realizado por: Carolina Valdiviezo

ANÁLISIS

Como mencionamos anteriormente se mantienen soportes de información dentro de la empresa pero esta no es actualizada correctamente ni mantiene soportes externos que ayude a la recuperación de datos en caso de enfrentar riesgos graves.

ANÁLISIS GENERAL DEL COMPONENTE: MONITOREO

SUMATEX mantiene controles y registro de las actividades y operaciones que se realizan pero es necesaria la mejora continua de estos ya que las medidas de control no siempre van a resultar eficientes ante los cambios constantes del medio.

ANEXO 3

NIVEL DE CONFIANZA Y NIVEL DE RIESGO
COMPONENTE 1: Ambiente Interno

Ponderación total de la encuesta

SI =	137
NO =	88

Total = 137+88=225 **Fuente:** (Anexo 3 Componente 1)

CALIFICACIÓN TOTAL

NIVEL DE CONFIANZA = ——————————

PONDERACIÓN TOTAL

NIVEL DE CONFIANZA = 137/225

NIVEL DE CONFIANZA = 0.61 ⟶ 61%

Tabla Nº 12: Ambiente Interno

⟵ **RIESGO DE CONTROL** ⟶

ALTO	**MODERADO**	**BAJO**
15 – 50 %	51 – 75 %	76 – 95 %
BAJO	**MODERADO**	**ALTO**

⟵ **NIVEL DE CONFIANZA** ⟶

El nivel de confianza obtenido se encuentra en un grado moderado lo que resulta tener también un grado de riesgo de control moderado.

COMPONENTE 2: Establecimiento de Objetivos

Ponderación total de la encuesta

SI =	130
NO =	95

Total = 130+95=225 **Fuente:** (Anexo 3 Componente 2)

CALIFICACIÓN TOTAL

NIVEL DE CONFIANZA = ——————————

PONDERACIÓN TOTAL

NIVEL DE CONFIANZA = 130/225

NIVEL DE CONFIANZA = 0.58 ⟶ 58%

Tabla Nº 13: Establecimiento de objetivos

⟵ **RIESGO DE CONTROL** ⟶

ALTO	**MODERADO**	**BAJO**
15 – 50 %	51 – 75 %	76 – 95 %
BAJO	**MODERADO**	**ALTO**

NIVEL DE CONFIANZA

El nivel de confianza obtenido se encuentra en un grado moderado lo que resulta tener también un grado de riesgo de control moderado.

COMPONENTE 3: Identificación de Riesgos

Ponderación Total de la encuesta

SI =	106
NO =	119

Total = 106+119=225 **Fuente:** (Anexo 3 Componente 3)

$$\textbf{NIVEL DE CONFIANZA} = \frac{\text{CALIFICACIÓN TOTAL}}{\text{PONDERACIÓN TOTAL}}$$

NIVEL DE CONFIANZA = 106/225

NIVEL DE CONFIANZA = 0.47 ⟶ 47%

Tabla Nº 14: Identificación de riesgos

RIESGO DE CONTROL

ALTO	**MODERADO**	**BAJO**
15 – 50 %	51 – 75 %	76 – 95 %
BAJO	**MODERADO**	**ALTO**

NIVEL DE CONFIANZA

El nivel de confianza obtenido se encuentra en un grado bajo, por ende da como resultado un nivel de riesgo de control alto.

COMPONENTE 4: Evaluación de Riesgos

Ponderación Total de la encuesta

SI =	28
NO =	32

Total = 28+32=60 **Fuente:** (Anexo 3 Componente 4)

$$\textbf{NIVEL DE CONFIANZA} = \frac{\text{CALIFICACIÓN TOTAL}}{\text{PONDERACIÓN TOTAL}}$$

NIVEL DE CONFIANZA = 28/60

NIVEL DE CONFIANZA = 0.47 ⟶ 47%

Tabla Nº 15: Evaluación de riesgos

RIESGO DE CONTROL

ALTO	**MODERADO**	**BAJO**
15 – 50 %	51 – 75 %	76 – 95 %
BAJO	**MODERADO**	**ALTO**

NIVEL DE CONFIANZA

El nivel de confianza encontrado es bajo, por lo que resulta un grado de riesgo de control alto.

COMPONENTE 5: Respuesta al Riesgo

Ponderación Total de la encuesta

SI =	38
NO =	37

Total = 38+37=75 **Fuente:** (Anexo 3 Componente 5)

$$\textbf{NIVEL DE CONFIANZA} = \frac{\text{CALIFICACIÓN TOTAL}}{\text{PONDERACIÓN TOTAL}}$$

NIVEL DE CONFIANZA = 38/75

NIVEL DE CONFIANZA = 0.51 ⟶ 51%

Tabla Nº 16: Respuesta al riesgo

RIESGO DE CONTROL

ALTO	**MODERADO**	**BAJO**
15 – 50 %	51 – 75 %	76 – 95 %
BAJO	**MODERADO**	**ALTO**

NIVEL DE CONFIANZA

El nivel de confianza objetivo se encuentra en un grado moderado lo que resulta tener también un grado de riesgo de control moderado.

COMPONENTE 6: Actividades de Control

Ponderación Total de la encuesta

SI =	230
NO =	145

Total = 230+145=375 **Fuente:** (Anexo 3 Componente 6)

$$\textbf{NIVEL DE CONFIANZA} = \frac{\text{CALIFICACIÓN TOTAL}}{\text{PONDERACIÓN TOTAL}}$$

NIVEL DE CONFIANZA = 230/375

NIVEL DE CONFIANZA = 0.61 ⟶ 61%

Tabla Nº 17: Actividades de control

RIESGO DE CONTROL

ALTO	**MODERADO**	**BAJO**
15 – 50 %	51 – 75 %	76 – 95 %
BAJO	**MODERADO**	**ALTO**

NIVEL DE CONFIANZA

El nivel de confianza objetivo se encuentra en un grado moderado, lo que resulta tener también un grado de riesgo de control moderado.

COMPONENTE 7: Información y Comunicación

Ponderación Total de la encuesta

SI =	155
NO =	160

Total = 155+160=315 **Fuente:** (Anexo 3 Componente 7)

$$\textbf{NIVEL DE CONFIANZA} = \frac{\text{CALIFICACIÓN TOTAL}}{\text{PONDERACIÓN TOTAL}}$$

NIVEL DE CONFIANZA = 155/315

NIVEL DE CONFIANZA = 0.49 ⟶ 49%

Tabla Nº 18: Información y comunicación

RIESGO DE CONTROL

ALTO	**MODERADO**	**BAJO**
15 – 50 %	51 – 75 %	76 – 95 %
BAJO	**MODERADO**	**ALTO**

NIVEL DE CONFIANZA

El nivel de confianza obtenido es bajo, por lo que el grado de riesgo de control encontrado es alto.

COMPONENTE 8: Monitoreo

Ponderación Total de la encuesta

SI =	163
NO =	107

Total = 163+107=270 **Fuente:** (Anexo 3 Componente 8)

$$\textbf{NIVEL DE CONFIANZA} = \frac{\text{CALIFICACIÓN TOTAL}}{\text{PONDERACIÓN TOTAL}}$$

NIVEL DE CONFIANZA = 163/270

NIVEL DE CONFIANZA = 0.60 ⟶ 60%

Tabla Nº 19: Monitoreo

RIESGO DE CONTROL

ALTO	**MODERADO**	**BAJO**
15 – 50 %	51 – 75 %	76 – 95 %
BAJO	**MODERADO**	**ALTO**

NIVEL DE CONFIANZA

El nivel de confianza objetivo se encuentra en un grado moderado, lo que resulta tener también un grado de riesgo de control moderado.

ANEXO 4

FOTOGRAFÍAS:
PUNTOS DE VENTA

Fig. 01: Almacén 10 de Agosto

Fig. 02: Matriz La Merced

Fig. 03: Almacén España

Fig. 04: Almacén España

Fig. 05: Oficina Administrativa

PROCESO DE PRODUCCIÒN

Fig. 06: Corte de tela

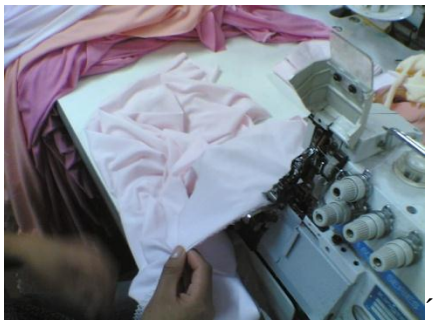


Fig. 07: Unión de hombros

Fig. 08: Unión de costados

Fig. 09: Bajo control de calidad

Fig. 10: Etiquetado y empaquetado

Fig. 11: Almacén exterior

MOLDES