UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE CONTABILIDAD Y AUDITORÍA

CARRERA DE CONTABILIDAD Y AUDITORÍA

Proyecto Integrador, previo a la obtención del Título de Licenciada en Contabilidad y Auditoría C.P.A.

Tema:

"Auditoría informática en la empresa Corporación Impactex Cía. Ltda. de la ciudad de Ambato"

Autora: Layedra Lagua, Soraya Belén

Tutora: Dra. Mg. Jiménez Estrella, Patricia Paola

Ambato – Ecuador

2022

APROBACIÓN DEL TUTOR

Yo, Dra. Mg. Patricia Paola Jiménez Estrella con cédula de identidad No. 1802934230, en mi calidad de Tutora del proyecto integrador sobre el tema: **"AUDITORÍA INFORMÁTICA EN LA EMPRESA CORPORACIÓN IMPACTEX CÍA. LTDA. DE LA CIUDAD DE AMBATO"**, desarrollado por Soraya Belén Layedra Lagua, de la Carrera de Contabilidad y Auditoría, modalidad presencial, considero que dicho informe investigativo reúne los requisitos, tanto técnicos como científicos y corresponde a las normas establecidas en el Reglamento de Graduación de Pregrado, de la Universidad Técnica de Ambato y en el normativo para presentación de Trabajos de Graduación de la Facultad de Contabilidad y Auditoría.

Por lo tanto, autorizo la presentación del mismo ante el organismo pertinente, para que sea sometido a evaluación por los profesores calificadores designados por el H. Consejo Directivo de la Facultad.

Ambato, Agosto 2022

TUTORA

Dra. Mg. Patricia Paola Jiménez Estrella

C.I. 180293423-0

DECLARACIÓN DE AUTORÍA

Yo, Soraya Belén Layedra Lagua con cédula de identidad No. 180499374-7, tengo a bien indicar que los criterios emitidos en el proyecto integrador, bajo el tema: **"AUDITORÍA INFORMÁTICA EN LA EMPRESA CORPORACIÓN IMPACTEX CÍA. LTDA. DE LA CIUDAD DE AMBATO"**, así como también los contenidos presentados, ideas, análisis, síntesis de datos, conclusiones, son de exclusiva responsabilidad de mi persona, como autora de este Proyecto Integrador.

Ambato, Agosto 2022

AUTORA

.....

Soraya Belén Layedra Lagua

C.I. 180499374-7

CESIÓN DE DERECHOS

Autorizo a la Universidad Técnica de Ambato, para que haga de este proyecto integrador, un documento disponible para su lectura, consulta y procesos de investigación.

Cedo los derechos en línea patrimoniales de mi proyecto integrador, con fines de difusión pública; además apruebo la reproducción de este proyecto integrador, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica potencial; y se realice respetando mis derechos de autora.

Ambato, Agosto 2022

AUTORA

.....

Soraya Belén Layedra Lagua

C.I. 180499374-7

APROBACIÓN DEL TRIBUNAL DE GRADO

El Tribunal de Grado, aprueba el proyecto integrador, sobre el tema: **"AUDITORÍA INFORMÁTICA EN LA EMPRESA CORPORACIÓN IMPACTEX CÍA. LTDA. DE LA CIUDAD DE AMBATO"**, elaborado por Soraya Belén Layedra Lagua, estudiante de la Carrera de Contabilidad y Auditoría, el mismo que guarda conformidad con las disposiciones reglamentarias emitidas por la Facultad de Contabilidad y Auditoría de la Universidad Técnica de Ambato.

Ambato, Agosto 2022

Dra. Mg. Tatiana Valle
PRESIDENTE

Dra. Rocío Cando
MIEMBRO CALIFICADOR

Dr. Joselito Naranjo
MIEMBRO CALIFICADOR

DEDICATORIA

Dedico este proyecto integrador principalmente a Dios , mi padre celestial por siempre protegerme, acompañarme en cada paso que doy y permitirme llegar a cumplir uno de mis objetivos.

A mi madre Beatriz Lagua, a la mujer que ha sido padre y madre para mí, por su constante apoyo e impulso al logro de todas mis metas, por ella es que estoy en el lugar que estoy, esta dedicatoria es una muestra que representa todo el esfuerzo que ella a echo por mi hermana y por mí, es un reflejo de los frutos que está cosechando, que ha formado una hija de bien.

Soraya Belén Layedra Lagua

AGRADECIMIENTO

En primer lugar, a Dios que me ha protegido en todo momento, al ser celestial que me ha dado sabiduría y entendimiento para guiar mi camino.

A mi madre Beatriz Lagua que ha estado siempre para mí en las buenas y las malas, siempre apoyándome en cada paso que doy, dándome ánimos para lograr los objetivos que me he propuesto. A mi hermana que ha sido la compañera de desvelos apoyándonos mutuamente en nuestros estudios. Gracias también a mi tutora la doctora Patricia Jiménez que fue una gran guia, compartiendo sus conocimientos, y así lograr con el cumplimiento del presente proyecto.

Así mismo a la compañía Corporación Impactex por la apertura y proporcioname toda la información requerida para este proyecto. Y por último y no menos importante agradecer a mis amigas por todos los consejos y apoyo.

Soraya Belén Layedra Lagua

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE CONTABILIDAD Y AUDITORÍA

CARRERA DE CONTABILIDAD Y AUDITORÍA

TEMA: "AUDITORÍA INFORMÁTICA EN LA EMPRESA CORPORACIÓN IMPACTEX CÍA. LTDA. DE LA CIUDAD DE AMBATO"

AUTORA: Soraya Belén Layedra Lagua

TUTORA: Dra. Mg. Patricia Paola Jiménez Estrella

FECHA: Agosto 2022

RESUMEN EJECUTIVO

El proyecto integrador tiene la finalidad de verificar el cumplimiento de los controles en las TIC, para ello se obtuvo la información física y digital por parte de los jefes de cada departamento analizado (financiero, marketing y sistemas) previamente autorizado por los directivos de la compañía. A partir de la información recolectada se da inicio con la planificación desde la aplicación de la entrevista en la visita preliminar, donde se pudo identificar en forma general el estado en el que se encontraba la empresa en cuanto a las tecnologías de información y comunicación. En segundo lugar, se realizó la ejecución de la auditoria a través de una encuesta marco COSO 2013 para detectar los principales riesgos en sus controles, también el desarrollo del mapa de calor en el que se identificó amenazas y vulnerabilidades principalmente de los activos de información. Como última fase se redactó un informe general de auditoria de sistemas. Entre los principales resultados podemos detectar que la empresa tiene el principal riesgo en el factor humano ya que no tiene fijado las funciones y responsabilidades de acuerdo a su área de trabajo. Así también se identificó que en los departamentos de finanzas y sistemas no se analiza los impactos de los riesgos para el cumplimento de los objetivos. A pesar de esto la compañía presenta una adecuada verificación del cumplimiento de controles.

PALABRAS DESCRIPTORAS: AUDITORÍA INFORMÁTICA, USO DE LAS TECNOLOGÍAS, SECTOR TEXTIL, METODOLOGÍA COSO 2013.

TECHNICAL UNIVERSITY OF AMBATO

FACULTY OF ACCOUNTING AND AUDITING

ACCOUNTING AND AUDITING CAREER

TOPIC: "COMPUTER AUDIT IN THE COMPANY CORPORATION IMPACTEX CÍA. LTDA. FROM THE CITY OF AMBATO".

AUTHOR: Soraya Belén Layedra Lagua

TUTOR: Dra. Mg. Patricia Paola Jiménez Estrella

DATE: August 2022

ABSTRACT

The purpose of the integration project is to verify compliance with ICT controls, for which physical and digital information was obtained from the heads of each department analyzed (financial, marketing and systems) previously authorized by the company's directors. Based on the information collected, planning began with the application of the interview in the preliminary visit, where it was possible to identify in general the state of the company in terms of information and communication technologies. Secondly, the execution of the audit was carried out through a COSO 2013 framework survey to detect the main risks in their controls, also the development of the heat map in which threats and vulnerabilities were identified mainly of information assets. As a last phase, a general systems audit report was drafted. Among the main results we can detect that the company has the main risk in the human factor since it has not set the roles and responsibilities according to their work area. It was also identified that the finance and systems departments do not analyze the impacts of the risks for the fulfillment of the objectives. Despite this, the company has an adequate verification of compliance with controls.

KEYWORDS: COMPUTER AUDIT, USE OF TECHNOLOGIES, TEXTILE SECTOR, COSO 2013 METHODOLOGY.

ÍNDICE GENERAL

CONTENIDO **PÁGINA**

PÁGINAS PRELIMINARES

ÍNDICE DE TABLAS

CONTENIDO **PÁGINA**

ÍNDICE DE FIGURAS

CONTENIDO **PÁGINA**

ÍNDICE DE ANEXOS

CONTENIDO **PÁGINA**

CAPÍTULO I

MARCO TEÓRICO

1.1 Introducción

1.1.1 Antecedentes del proyecto integrador

Los antecedentes del presente proyecto integrador han sido tomados de Vélez (2022) Ingeniero en Sistemas, colaborador de empresa Corporación Impactex cía. Ltda.

1.1.1.1 Historia de la empresa

Impactex nace en la cuidad de Ambato en agosto del año 1999 su propietario el señor Milton Altamirano y su esposa Martha segura, inician sus actividades en el sector textil confeccionando y produciendo ropa interior masculina y camisetas unisex. En el transcurso de los primeros años fue ganando aceptación con sus clientes, generando el incremento de su producción, siendo el inicio para diversificar su línea de productos.

La visión y emprendimiento del señor Altamirano marca la pauta para que la ropa interior tenga una identidad propia, con calidad en las materias primas, diseños innovadores y a la moda que generen más consumidores, introduciéndose al mercado femenino y de niños.

Actualmente Impactex siendo fiel a su política de calidad, crea sus propias marcas legalmente patentadas, con el valor agregado de satisfacer las necesidades de sus clientes, tales como:

- Marca Mao
- Marca impacto
- Marca leidy Jasmín
- Marca mao junior e impactito
- Marca verito´s

1.1.1.2 Detalles estratégicos

MISIÓN

Somos una organización dedicada a la Innovación desarrollo y comercialización de marcas de moda con excelencia posicionándonos en los mercados nacionales y extranjeros para generar rentabilidad, sostenibilidad y crecimiento empresarial para nuestros clientes internos y externos.

VISIÓN

Ser un grupo empresarial líder en el mercado de moda con excelencia, responsabilidad social, empresarial y ambiental, internacionalizando nuestras marcas para crecer y consolidarnos, con nuestros consumidores neo tradicionales casuales.

OBJETIVO EMPRESARIAL

Generar recursos económicos por medio del desarrollo y la comercialización del portafolio de productos de Marcas, para satisfacer necesidades de vestimenta y estilo neo tradicional del mercado nacional e internacional.

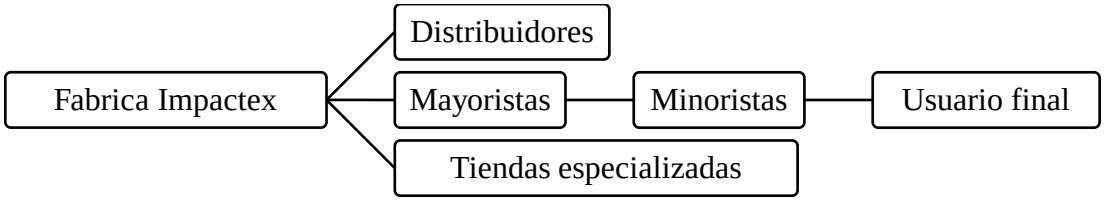
OBJETIVO COMERCIAL

Comercializar prendas de ropa interior acordes a la moda, marcando la diferencia del buen vestir interior en el mercado nacional.

CANAL DE COMERCIALIZACIÓN

Impactex tiene definido su canal de comercialización siguiendo el siguiente esquema

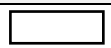
Figura 1. Esquema de comercialización



Fuente: Vélez (2022)

1.1.1.3 Estructura organizacional

Figura 2. Estructura organizacional

Cuadro de Referencia	
Símbolo	**Significado**
	Proceso, Departamento
	Línea conectora de elementos

Fuente: Vélez (2022)

1.1.1.4 Detalles de operación

El objeto empresarial de la compañía consiste en dedicarse por cuenta propia o terceros a la producción, elaboración, terminado de manera directa o por medio de la modalidad de maquila. Además, de la comercialización, distribución, importación de otras marcas, exportación, de todo tipo de textiles, prendas de vestir o de bioseguridad al por mayor y menor.

1.1.1.5 Detalles legales

Se rigen bajo normativas legales vigentes establecidas en la Constitución del Ecuador, Ley de Régimen Tributario Interno, Reglamento para la aplicación de la Ley de régimen tributario Interno, Código de trabajo, Ley de la Propiedad Intelectual y supervisado por la Superintendencia de Compañías.

1.1.1.6 Marcas y logos

A continuación, se detalla las marcas de mayor éxito de la empresa:

Marca Mao.- ropa interior para hombres de algodón con sus líneas bóxer, calzoncillos, camisetas, dividís marca que actualmente lidera el mercado nacional y con miras de exportación a países como Perú y Colombia.

Marca impacto: para el segmento masculino en poli algodón de precios medios económicos en líneas como bóxer calzoncillo tanga y dividí.

Marca leidy Jasmín: ropa interior para mujeres con estilos acordes a la moda prendas confortables con gran dedicación y calidad

Marca mao junior e impactito : para el segmento infantil de niños con coloridos diseños y atractivos modelos que son cada vez más aceptados para la sociedad

Marca verito´s: Ropa interior para niñas con toques de delicadeza y variedad de diseños que cuidan la ternura de la infancia.

IMPACTEX: Logo principal de la compañía.

1.1.1.7 Ubicación

La compañía CORPORACIÓN IMPACTEX CÍA. LTDA. Se encuentra ubicada en la Av. 22 de Enero y Circunvalación a 200 metros de la entrada a la parroquia Atahualpa junto al Complejo REVOLUTION en la ciudad de Ambato de la provincia de Tungurahua.

Contactos

Teléfonos: 593 (03) 2450600 / (03) 2855704 / (03) 2452961

· Ventas: ventas@impactexmao.com

· Publicidad y eventos: marketing@impactexmao.com

· Compras a proveedores: compras@impactexmao.com

· Cobranzas y créditos: creditosycartera@impactexmao.com

1.1.1.8 Contextualización del problema

CORPORACIÓN IMPACTEX CÍA. LTDA. gracias al crecimiento en sus ventas, vio la necesidad de obtener mejoramiento en su tecnología e información empresarial, en la visita previa a la institución se evidencio debilidades en ciertos controles internos; segregación de funciones, seguridad de la información y autenticidad de seguridad de datos y aplicación de controles medios.

1.1.2 Descripción del entorno

1.1.2.1 Necesidad la auditoría informática como herramienta para la verificación y validación de controles en las organizaciones

Rodríguez Labrada et al. (2019) afirman que actualmente la auditoria informática es necesaria en las organizaciones, ya que da paso a la evaluación de sus recursos de información y el uso de los mismos. Se enfocan en la evaluación de la estructura interna así mismo de los procesos y apoyo estructural. Del mismo modo, tener modelos de ciberseguridad como soporte en el desarrollo de la auditoria, a través de dominios efectivos para la evaluación de controles y respuestas a posibles amenazas cibernéticas (Sabillón & Cano, 2019).

En América Latina Yetano & Castillejos (2019) concluyen que la auditoria tiene un limitado desarrollo ya sea por motivos políticos o económicos que impiden el desenvolvimiento de técnicas avanzadas. Sin embargo, Faúndez et al. (2018) afirman que los procesos de auditoria no son iguales, demuestran que tienen un tratamiento asimétrico en algunos países aplican la auditoria a través de sistemas electrónicos mientras que en los demás incluyendo a Ecuador no lo utilizan.

Es importante conoce del sector y la actividad que desarrolla la entidad que será auditada, esta información en especial el control operacional y la gestión financiera se obtiene con facilidad gracias al apoyo de sistemas informáticos (Paredes & León, 2021).

1.1.2.2 Planificación de la auditoria informática para la evaluación de gestión de las tic en el sector textil ecuatoriano

La auditoría informática faculta a las organizaciones alinearse a los estándares internaciones de la utilización correcta de las tecnologías de la información, por ello, una adecuada planificación determina que los procesos no sean cuestionado por las partes involucradas (Arcentales & Caycedo, 2017). De este modo, Espinoza et al. (2020) aseguran que el adecuado desarrollo de la auditoria informática apoyaría a que la organización pueda actualizarse en los procesos tradicionales tanto en la evaluación y gestión de riesgos.

Generalmente en la etapa de planificación de auditoria optan por la utilización de la metodología COBIT 5, que esta direccionada al cumplimiento de estrategias de la organización. Para Jimbo et al. (2017) esta metodología es efectiva puesto que involucra a toda la organización más allá de su rol, está encaminado al logro de objetivos, controles generales de las TI en sus procesos y aplicación. Inclusive, Santacruz et al. (2017) mencionan que la principal ventaja es la optimización de recursos de los sistemas informáticos.

La auditoría informática tiene un rol esencial en las organizaciones acorde a las operaciones y al sector que permanezca, con fines informáticos y tecnológicos (Bailon, 2019).

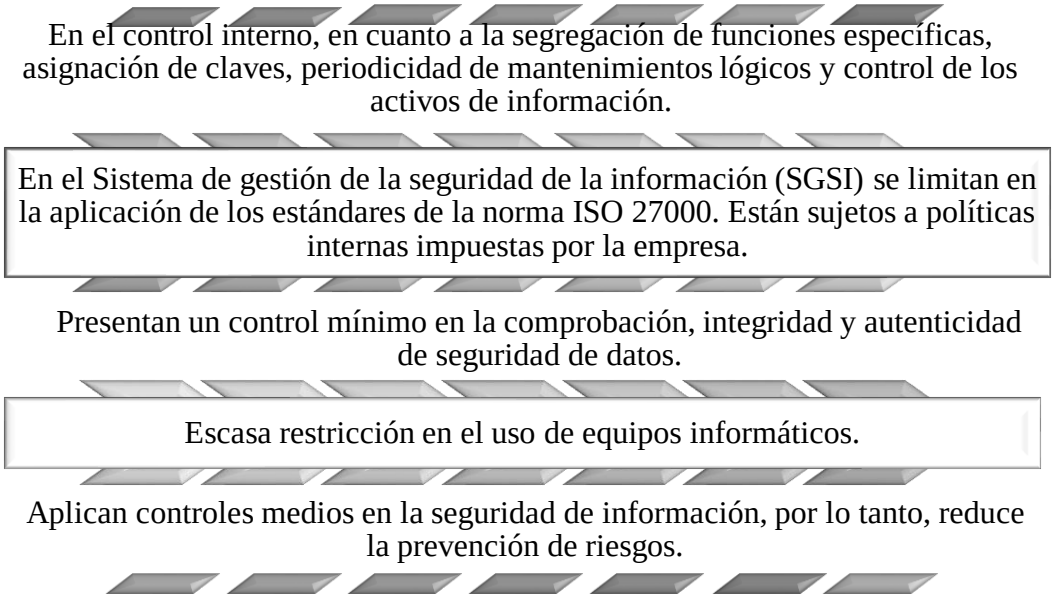
1.1.2.3 Delimitación de la necesidad de la organización

CORPORACIÓN IMPACTEX CÍA. LTDA. con siete años en el mercado ha logrado destacarse con la marca internacional MAO. Gracias a la inversión que han tenido en la misma; en su imagen, presentación, diseño y calidad generalmente enfocados en el segmento deportivo. Llegando a gran parte del mercado del Ecuador.

Actualmente trabajan internacionalmente con la marca en México, Estados Unidos y Canadá, día a día buscan nuevos mercados en el ecuador para su crecimiento. Con el crecimiento en sus ventas, gerencia vio la necesidad de implementar maquinaria especial para satisfacer la demanda. Adquieren maquinaria nueva bajo la aprobación del departamento financiero y socios de la Compañía para producir prendas con costura plana y la maquinaria en exceso de la planta de producción fue ofertada.

Debido a que trabajan con tecnología de punta y en busca del bienestar de empleados y clientes han implementado controles internos. En la visita preliminar a la compañía se evidencia debilidad en ciertos controles en el área informática, entre ellos:

Figura 3. Debilidades en las TIC de la compañía

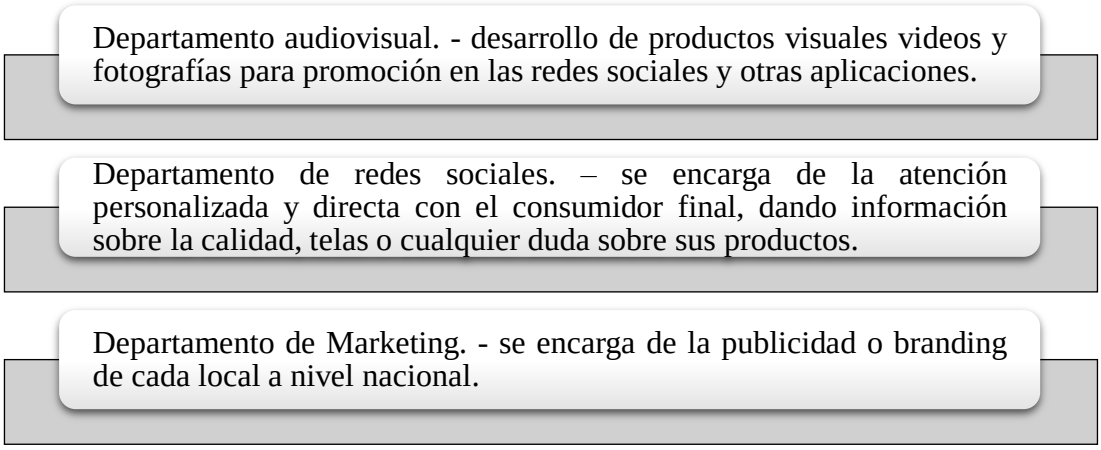


Elaborado por: Layedra (2022)

En importante considerar que la compañía está creando una página web de venta en línea (e-commerce) y sistemas propios. Además, se menciona que la compañía no ha realizado auditorías informáticas en años anteriores.

Adicionalmente implementaron nuevos departamentos que ha logrado satisfacer las necesidades de los clientes y lograr un reconocimiento en el mercado teniendo un contacto directo con ellos.

Figura 4. Departamentos nuevos e la organización



Elaborado por: Layedra (2022)

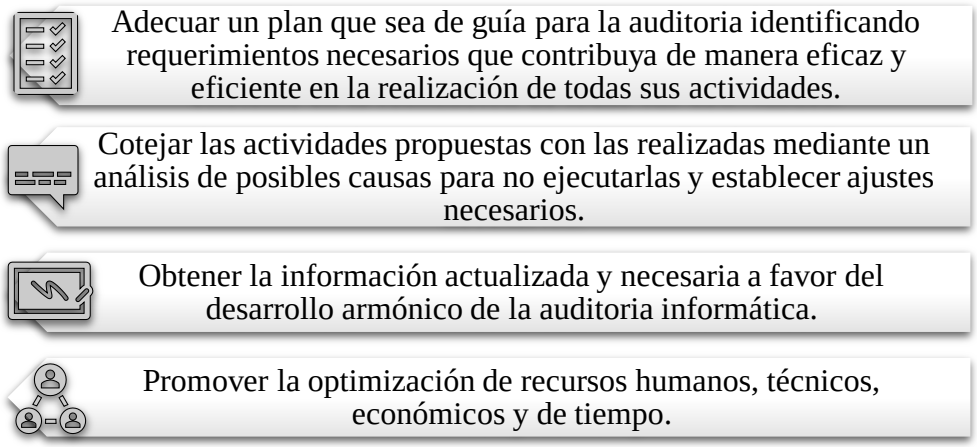
Departamento Community managment. – genera el contenido de Facebook e Instagram de Ecuador, Estados Unidos y Canadá, además, de gestionar pedidos internacionales.

1.1.3 Justificación

La auditoría informática es una herramienta de gestión estratégica, al momento de ejecutar un proceso desde la fase inicial (planeación) a la fase final (revisión o evaluación) (I Aumatell, 2013).

Los principales objetivos de una planeación de auditoria Informática son:

Figura 5. Objetivos de la planeación de Auditoría Informática



Fuente: Tamayo & Duque (1999)

Elaborado por: Layedra (2022)

Una correcta gestión de la tecnología informática abarca los conocimientos que permiten el diseño y construcción de los sistemas informáticos, estos sistemas constan de una parte física; máquinas de los diferentes ordenadores y las conexiones entre ellas, además, conformada de otra parte; conjunto de programas conocidos genéricamente como el hardware y software, la tecnología se asocia con las dos partes (Marco et al., 2012). Los sistemas de información se encargan de la recolección, tratamiento y uso de la información siendo un apoyo en las actividades humanas (Davies, 2014).

Con ello, este tipo de auditoria se llevó a cabo a través de la evaluación de los equipos de cómputo, de un sistema o de un procedimiento especifico, la evaluación se realizará desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información. Se debe incluir equipos de cómputo como una herramienta para la obtención de la información y con una organización adecuada (Tamayo Alzate, 1999).

Los procedimientos dados en la auditoría buscan anticipar las evoluciones principales de la actividad informática tanto en los programas básicos, programas de aplicaciones, recursos humanos (Derrien, 2009). Se consideró que la estructura de un plan informático tenga la consideración de la evolución continua que tiene la tecnología.

Como afirman Ocaña Fernández et al. (2020) la gestión de las tecnologías es un esquema fundamental en la innovación tecnológica aportando a la mejora sustantiva en la calidad de los servicios que ofrece la compañía.

El proyecto integrador permitió la aplicación de técnicas y procedimientos que garantizaron la confiabilidad de los hechos encontrados y se pudo determinar el estado real en la aplicación de controles sobre las tecnologías de información y comunicación utilizadas por la compañía. Además, se pudo analizar aspectos positivos y negativos desde la instalación de nuevas tecnologías, en la contratación de personal, desarrollo de software, comprobación y el estado de instalaciones para garantizar la seguridad, periodicidad de controles y establecimiento de los mismos.

Para el cumplimiento de los objetivos mencionados en el trabajo, se aplicó herramientas como entrevista, cuestionario para la recolección de información requerida en el diagnóstico de los controles implementados por la empresa en cuanto al uso de las TIC. Con la aplicación de la técnica de observación, pruebas de

conformidad y pruebas sustantivas, se facilitó el acceso a la información de la compañía, tomadas de fuente primaria.

Con el desarrollo del proyecto integrador se evidenció la importancia que tiene en la organización, realizar una auditoria informática con el fin de mejorar y elevar el valor de la compañía proporcionando aseguramiento y análisis sobre los posibles riesgos, principios de integridad, competencia y diligencia profesional que beneficia la evaluación, seguimiento y monitoreo en el adecuado uso de las TIC.

El auditor debe ser objetivo e independiente para lograr una comunicación de los resultados en pro de la mejora continua y recomendación de posibles estrategias a favor de la compañía (Barberán Arboleda & Díaz Díaz, 2019).

1.1.4 Objetivos

Objetivos General

Ejecutar la auditoría informática a la Empresa Corporación Impactex Cía. Ltda. de la ciudad de Ambato para la verificación del cumplimiento de controles en las TIC.

Objetivos Específicos

- Elaborar la planificación de la auditoría informática para la evaluación de controles de las TIC.
- Ejecutar la auditoría informática con la aplicación de programas y papeles de trabajo para la obtención de evidencias que permitan la sustentación de resultados.
- Comunicar a través de la emisión del informe de auditoría informática las conclusiones y recomendaciones con respecto a los controles de las TIC.

1.2 Revisión de la literatura

1.2.1 La teoría de la organización - contingencia y la auditoria informática en las organizaciones

La teoría de contingencia es en las organizaciones en el que se produce diversas ideas y mantiene el apoyo de sus colaboradores, es la base de lo mucho que sé que se aplica en la actualidad (Donaldson , 2001). Por ello al emplear esta teoría de contingencia en

el desarrollo de la auditoria informática, se puede analizar los aspectos positivos y negativos de las decisiones tomadas por los altos mandos.

Con esta teoría podremos determinar si la organización requiere de cambios sobre la administración de la organización, así también, sobre el factor humano, estructura o prácticas laborales y que la empresa tenga éxito con las decisiones tomadas.

Para una correcta estructuración y presentación de los resultados en conjunto de la auditoria se hace referencia a la norma IEEE tiene por objetivo la importancia de los derechos de autor y la forma en la que se evita el plagio haciendo una presentación estructurada, todo esto orientado para el desarrollo de citas y referencias bibliográficas (Ignacio Tebar, 2016).

1.2.2 Concepto de auditoría

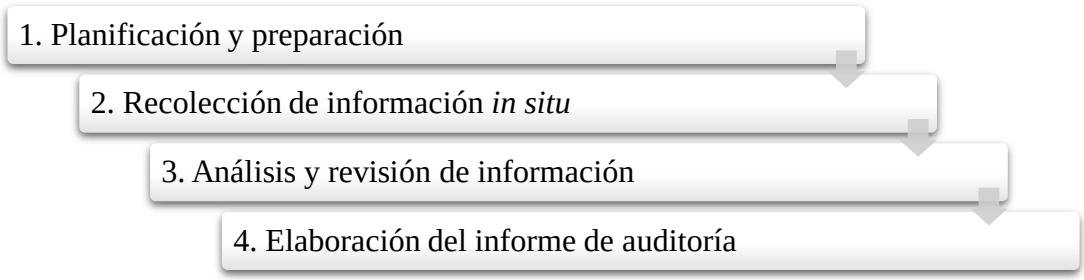
La Auditoría proviene del latín auditorios, es la virtud de revisar las cuentas, orientadas a la evaluación de la economía, eficiencia y eficacia con el uso de los recursos, siendo un examen objetivo y sistemático de las operaciones financieras, realizado posterior a la ejecución (cierre del ejercicio), desarrollada especialmente por personal independiente a las operaciones de la organización, con el fin de evaluarlas y elaborar un informe que incluirá comentarios, recomendaciones y conclusiones (Armas, 2008). Así mismo para Sánchez (2021) la auditoría es una técnica, que en sus diferentes áreas tiene un objetivo y propósito, enfocadas en realizar la evaluación bajo un criterio y determinar la conformidad de los hechos pasados.

Vila (2007) define a la auditoria bajo la norma ISO 8402, como un examen metódico que se desarrolla para determinar si las operaciones y los resultados cumplen con las disposiciones de forma adecuada para alcanzar los objeticos de la organización.

1.2.3 Fases de la auditoría

El proceso de auditoria se diferencia en cuatro fases generales:

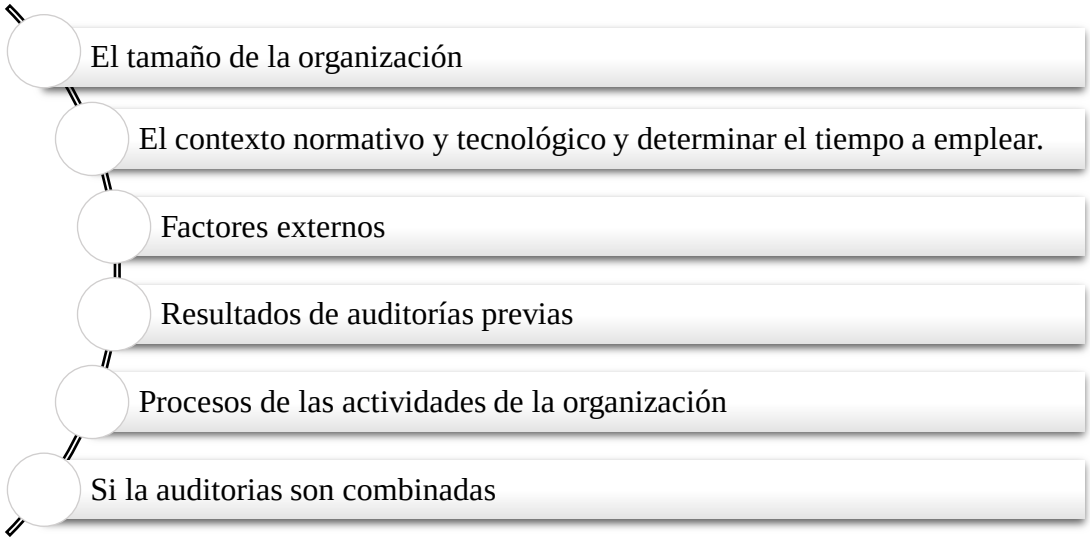
Figura 6. Fases de la Auditoria de Sistemas



Fuente: Couto Lorenzo (2020)
Elaborado por: Layedra (2022)

La primera fase es fundamental en la auditoría, para que, en el momento de ejecución de la misma, se desarrolle de forma fluida y que sea efectiva.

Figura 7. Consideraciones para la planificación

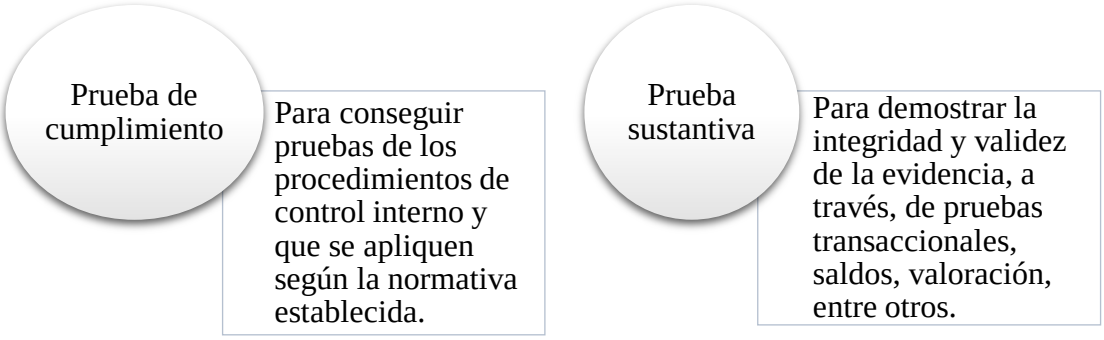


Fuente: Sevilla (2015)
Elaborado por: Layedra (2022)

Tiene la finalidad de organizar e informar las actividades a realizar por el equipo de auditoria, para acordar las fechas de realización con anticipación.

La segunda fase es la más visible de la auditoria, genera mayor interacción entre los integrantes del equipo de auditoría, recaban información; del tamaño de la organización, sector al que pertenece, productos que elabora, leyes y normas que aplica, tecnología que emplea, y otra información que complementaria, considerando los objetivos y alcance de la organización.

Figura 8. Tipos de prueba



Fuente: Abolacio (2018)

Elaborado por: Layedra (2022)

Una vez reunida la información, empieza la tercera fase, en la que se reúne el equipo de auditoria para dar inicio del análisis y evaluación de la misma, determinando las observaciones y hallazgos por cada uno de los miembros. El quipo auditor comprobara si dichos hallazgos están suficientemente apoyados de la suficiente evidencia. Así mismo Salas (2007) indica que los auditores revisaran las evidencias bajo las normas, que corroboraran la seguridad y fiabilidad de la misma, el número de reuniones que tendrá el equipo de auditoria dependerá del tamaño de la organización.

En la última fase de elaboración de informes, es la responsabilidad del auditor líder, basados en los papeles de trabajo, el auditor redactara el informe, con el objetivo de dar a conocer de forma precisa los resultados de la auditoría y el contexto en el que se llevó a cabo. El auditor realizara primero un informe borrador, que lo presentara al equipo de auditoria para su revisión y realizar posibles correcciones, para la presentación del informe final. Como lo indica López (2020) en términos de las NIA, lo denomina como informe de auditoría, que anteriormente según las normas derogadas del año 2013 se lo conocía como dictamen sobre los estados financieros, el informe contendrá el resultado de la auditoria de un solo estado o un elemento, cuenta o de los estados financieros resumidos.

1.2.4 Auditoría informática

1.2.4.1 Definición

Para Sánchez (2021) está encaminada a la evaluación de riesgos y controles, sobre la seguridad de los sistemas de información, niveles de seguridad, en cada etapa, con el fin de examinar los datos, información, conocimientos, equipos (hardware) y

aplicativos (software) y determinar si han sido objeto de manipulación o de haber sufrido alguna alteración. Los criterios de evaluación de seguridad y la integridad de la información, pueden ser los estándares internacionales o con el enfoque Cobit, Cobit es un modelo utilizado en la auditoria enfocado en la gestión y el control de los sistemas informáticos y tecnológicos, también, puede tener un enfoque sobre los sistemas de información de manera general, calidad y seguridad general de los datos.

Es un proceso encargado de la recolección, agrupación y evaluación de las evidencias para determinar si tal sistema informático salvaguarda los activos de información, en el que permanece la integridad de datos, el cumplimiento de los respectivos fines de la empresa, utilizando menor cantidad de recursos (Piattini et al., 2015).

1.2.4.2 Objetivo

Verificar la fiabilidad de herramientas informática en consecuencia el manejo de los mismos, la complejidad de este objetivo a que se emplee una cadena de procesos, que asegure al auditor la fiabilidad de la información que esta evaluado, a pesar de la constante evolución de la informática, es posible contar con la documentación necesaria, por ello se sintetiza en que, un buen programa de información no es aquel que no tenga fallos, más bien, es aquel que no tiene fallos de carácter grave (Derrien, 2009).

1.2.4.3 Aspectos que debe dominar el auditor informático

Los conocimientos informáticos que posee el auditor son un papel muy importante, por ello expone una serie de aspectos que debe dominar para realizar sus funciones:

Tabla 1. Aspectos que debe dominar el Auditor

Informática básica	➢ Sistemas operativos que utiliza la entidad, conocimientos generales de hardware, computadores formatos de archivos, informática, redes de comunicación, etc. ➢ Procesadores de textos, gestores de base de datos, graficadores, etc.
Programación de computadoras	➢ Técnicas básicas. ➢ Lenguaje más conocido.

Base de datos	➢ Conceptos y definiciones. ➢ Modelos actuales. ➢ Características de los gestores. ➢ Funciones y responsabilidades. ➢ Seguridad de la información.
Redes de computadoras	➢ Conceptos generales. ➢ Estructura básica. ➢ Sistemas operativos que estén en uso en la organización. ➢ Protección de la información en red.
Tecnología de diseño y elaboración de sistemas	➢ Conceptos y otras definiciones. ➢ Diseño de entradas y salidas de información, procesos automatizados, procedimientos manuales y controles informáticos. ➢ Preparar manuales. ➢ Metodología del trabajo bajo normas.
Seguridad y protección de información en entornos informatizados	➢ Protección física, organizativa, por software, instalación de equipos, dispositivitos, remodelaciones. ➢ Proceder ante virus informáticos y otros. ➢ Preparación de planes ante amenazas de tipo natural.
Técnicas criptográficas	➢ Conceptos de encriptación y desencriptación. ➢ Métodos generales. ➢ Especialización de software.
Redes globales de información	➢ Internet y servicios ➢ Softwares especializados.
Técnicas de auditoría apoyada de computadores.	➢ Método existentes ➢ Conocimientos en software específico y generales.
Comercio electrónico	➢ Modalidades ➢ Problemas de seguridad y protección de archivos. ➢ Firmas electrónicas. ➢ Normativa

Fuente: Blanco Encinosa (2008)

Elaborado por: Layedra (2022)

Todo el listado citado anteriormente son algunos de los conocimientos que debe poseer un auditor, aunque es amplio no es definitivo, en los temas de computación y comunicación están en un constante cambio, desarrollo que lo más posible es que haya que añadir nuevos elementos en un año. Así, como hay nuevos elementos que agregar, también, con el paso del tiempo algunos de estos se convierten en obsoletos.

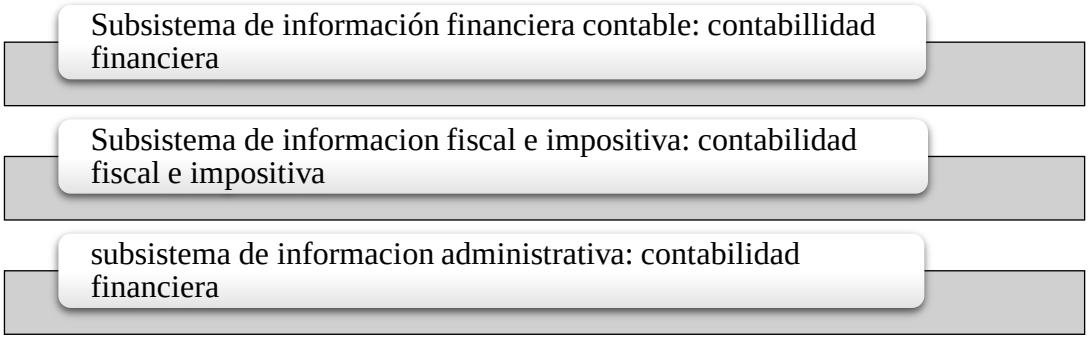
1.2.5 Sistemas de información

Un sistema de información está relacionado con los demás sistemas y con el entorno de la empresa, capaz de captar información que esta necesite y adaptarlas haciendo los cambios necesarios, en poder de los miembros de la empresa, ya sea en la toma de decisiones, control estratégico o en la ejecución de las decisiones adoptadas (Lapiedra et al., 2016).

1.2.6 Sistema de información contable

Lezanski et al. (2016) sostienen que es la idea general es proveer de información fiable a terceros, con el objetivo de facilitar la toma de decisiones, a los directivos, proveedores, economistas, inversionistas, entidades bancarias, entes de control y se dividen en subsistemas como se describe en la figura 9.

Figura 9. Subsistemas del sistema de información contable



Fuente: Lezanski et al. (2016)

Elaborado por: Layedra (2022)

1.2.7 Tipos de auditoría de sistemas de información

Se determina que la auditoría de sistemas de información conlleva la evaluación compleja de la organización, por ello esta se divide en varios tipos como se muestra en la tabla 2.

Tabla 2. Tipos de Auditoría

Auditoría informática de explotación	Analiza los resultados informáticos de cualquier tipo, en listados impresos o automatizados. Son sometidos a controles de calidad, a través de procesos correcto.

Auditoria informática de Sistemas Analiza las actividades relacionadas en el entorno informático.	**Sistemas operativos:** Comprueba si están actualizados, y las causas en caso de no estarlos. Se revisan incompatibilidades en el software.
	Software básico: analizan aplicaciones instaladas.
	Tunning: evalúan técnicas y comportamiento del sistema.
	Optimización de los sistemas y subsistemas: se comprobará si las acciones son efectivas, sin involucrar la operatividad.
	Administración de la base de datos: el auditor comprobara la seguridad, integridad y autenticidad de datos.
	Investigación y desarrollo: auditoria se mantendrá en la investigación y desarrollo, facilitando procesos y labores importantes.
Auditoría informática de comunicaciones y redes	Analiza los diferentes dispositivos, que son parte de las redes de la organización, para encontrar debilidades y proponer posibles correcciones. Los auditores deben tener conocimientos en tipos de red de comunicación, como los detalles, ubicación y operatividad.
Auditoría de desarrollo de proyectos	Loa auditores revisan la metodología que se utiliza para el desarrollo de los diferentes proyectos en la empresa, diferenciando cada área y a nivel global.
Auditoria de Seguridad Informática	Revisa los procesos de la seguridad informática, tanto físicos (hardware, dispositivos, instalaciones y entono) ante posibles catástrofes, y como lógicos (software, procesos y programación).

Fuente: Tejada (2015)
Elaborado por: Layedra (2022)

1.2.8 Metodología marco de referencia COSO

El marco de referencia COSO 2013 es un modelo de control interno conformado por cinco componentes que la administración dísela y aplica con el fin de garantizar seguridad razonable sobre el control que tienen en la compañía, es de gran apoyo para impedir y detectar errores materiales en cualquier área de la empresa.

Tabla 3. Componentes COSO

Componente	Descripción	Subdivisión (si procede)
Ambiente de control	Hechos, políticas y procedimientos que demuestran el proceder general de alta gerencia, directores y propietarios de la organización respecto al control y su importancia.	Integridad y valores, compromiso y valores éticos Participación de los directivos, filosofía operativa de la administración Estructura organizativa, asignación de autoridad y responsabilidades Políticas y prácticas de RH
Riesgo de evaluación	Definición y análisis a cargo de la administración sobre los riesgos en la preparación de estados financieros conforme a los principios contables generalmente aceptados.	Procesos: Identificación de factores que afecten los riesgos Evaluación de la importancia y probabilidad de ocurrencia de los riesgos Determinación de acciones
Actividades de control	Políticas y procedimientos que los admirativos establecieron para el cumplimiento de objetivos sobre los informes financieros.	Afirmaciones de la administración que deben ser satisfechas: Existencia u ocurrencia, Integridad, Valuación o asignación, Derecho y obligaciones, Presentación y manifestación
Información y comunicación	Métodos utilizados para identificar, reunir, clasificar, registrar y comunicar sobre las actividades de la organización y para conservar la contabilidad de activos relacionados.	Tipos específicos de actividades de control: Separación adecuada de tareas Autorización de operaciones Documentación y registros adecuados Control físico de los activos y archivos Verificaciones independientes para el desempeño
Monitoreo	Evaluación continua y periódica por la administración cuanto a la eficacia y funcionamiento de la estructura del control interno para establecer si hay funcionamiento conforme a los objetivos y si es necesario modificarlo.	N/A

Fuente: Arens, Mark S., & Randal (2007)

Elaborado por: Layedra (2022)

1.2.9 SAS las declaraciones de normas de auditoría

Estas normas son emitidas por la Junta de Normas de Auditoria convirtiéndose en una guia para los auditores externos acerca de control interno durante la aplicación de una auditoria financiera así también de la eficiencia de sus actividades y del cumplimiento de las normas (Bejarano, s.f.).

1.2.10 Norma internacional de auditoría 401

Basado en esta NIA determina que el auditor debe considerar el ambiente SIC (sistemas de contabilidad y de control interno) durante el procedimiento de auditoria con el objetivo de reducir el riesgo en su aplicación, el alcance de la auditoria no cambia ya sea porque los datos sean procesados de forma manual o computarizada, ya que el auditor pone en práctica diferentes métodos y técnicas con el apoyo de computadoras, manuales o su combinación con el fin de obtener evidencia suficiente (Ignacio Tebar, 2016).

1.2.11 Normas ISO (International Standarization Organization)

La ISO es una organización Internacional de estandarización no gubernamental sin fines de lucro fundada el 2 de febrero de 1947 que fomenta el desarrollo e implantación de normas a una organización tanto manufactureras como de servicio a nivel internacional, así también la ISO proporciona herramientas que favorecen el cumplimiento de objetivos tales como desarrollo de actividades tecnologías, científicas, económicas e intelectuales (Universidad EAFIT, 2017).

1.2.12 Series de clasificación de las normas ISO

Estas normas se clasifican en series diferentes que intentan estandarizar diversos temas, así como se muestra en la tabla 4.

Tabla 4. Clasificación de las normas ISO

Serie	Descripción
ISO 9000	Control y gestión de calidad
ISO 14000	Aspectos ambientales de productos y organizaciones
ISO 19000	Realización de auditorías internas y externas basado en la norma ISO 9001
ISO 27000	Estándares de seguridad de la Información
ISO 31000	Gestión de riesgos

Fuente: Universidad EAFIT (2017)
Elaborado por: Layedra (2022)

1.2.12.1 ISO 9001 sistemas de gestión de la calidad

Es importante que una organización tenga una gestión de calidad eficaz, el pensamiento basado en riesgos ayudara que las organizaciones tengan acciones preventivas y la toma de acciones adecuadas para la prevención de ocurrencia de posibles riesgos (ISO, 2015).

1.2.12.2 ISO 27001 :2013 guia de implantación para la seguridad de información

Esta norma es un marco para la protección de la información que es adaptable a organizaciones de cualquier tipo y tamaño, por ello es que las organizaciones eligen la implantación de los sistemas de gestión de seguridad de la información y que se cumpla la norma ISO 27001 (ISO, 2013).

1.2.13 Normas de control interno

La ley orgánica de la Contraloría General del Estado dispone la regulación del sistema de control adaptado a las normas de control interno, a partir de este marco cada institución impartirá sus normas, políticas y manuales acorde a las necesidades en su gestión, estas normas están compuestas por; normas generales y otras relacionadas a la administración financiera gubernamental, talento humano, tecnología de la información y administración de proyectos todos estos integrados al marco de control interno emitido por el comité de organizaciones (COSO), establecido por cinco componentes con el fin del cumplimiento de objetivos institucionales (Contraloría General del Estado, 2014).

1.2.13.1 Grupo 410 - tecnología de la información

Como lo establece la Contraloría General del Estado (2014) este grupo está compuesto por subgrupos tales como:

410-01 Organización informática
410-02 Segregación de funciones
410-03 Plan informático estratégico de tecnología
410-04 Políticas y procedimientos
410-05 Modelo de información organizacional

410-06 Administración de proyectos tecnológicos

410-07 Desarrollo y adquisición de software aplicativo

410-08 Adquisiciones de infraestructura tecnológica

410-09 Mantenimiento y control de la infraestructura tecnológica

410-10 Seguridad de tecnología de información

410-11 Plan de contingencias

410-12 Administración de soporte de tecnología de información

410-13 Monitoreo y evaluación de los procesos y servicios

410-14 Sitio web, servicios de internet e intranet

410-15 Capacitación informática

410-16 Comité informático

410-17 Firmas electrónicas

1.2.14 Tecnologías de la información y la comunicación

1.2.14.1 Evolución histórica

Pacheco (2016) describe la historia de la TIC de la siguiente forma:

En la década de los sesenta en el siglo XX comenzó con el planteamiento de una posibilidad de interconectar computadores y facilitar la comunicación en el mundo, se hizo investigaciones durante veinte años y en 1985, una red internacional conocida como Internet.

Se estableció como tecnología de investigación, con el uso de esta nueva tecnología, los computadores necesitaban del uso de un modem, una línea telefónica y por ende tener que contar con un proveedor de este servicio y poder conectarse a una red mundial. Para lograr la conexión debían realizar una llamada a dicho proveedor, creando una charla; envió y recepción de datos, una de las desventajas que tenía esta, fue que, no se podían realizar llamadas de forma simultánea con el uso del internet. En la actualidad se puede desarrollar diferentes actividades al mismo tiempo.

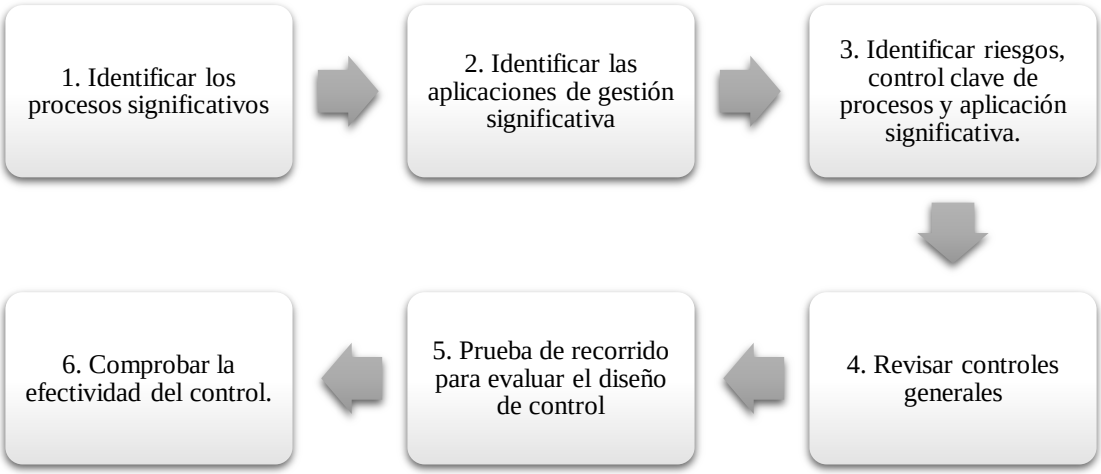
1.2.14.2 Definición

Morles (2001) citado por Peña (2011) lo define como la producción de objetos y procesos útiles para el ser humano, además de la aplicación de conocimientos científicos, para la resolución de problemas complejos, es decir, el saber hacer y saber su utilidad.

1.2.14.3 Procedimientos de revisión de las tecnologías de la información

La tecnología de la información está en constante evolución, por ello se requiere del personal especializado, para realizar su evaluación, de riesgo, a nivel de cuentas y realizar pruebas de control y la aplicación de procedimientos sustantivos adecuados.

Figura 10. Etapas de revisión general del control interno



Fuente: Instituto Mexicano de Contadores Públicos (2020)

Elaborado por: Layedra (2022)

1.2.14.4 Herramientas de información

Es importante considerar las herramientas de información que serán sujetas a la evaluación en el proceso de auditoria, tal como lo describe (Vasconcelos, 2016); aplicaciones de internet, acceso a la Web, URL dirección de páginas web, dominios y aplicaciones basadas en la web.

CAPÍTULO II

METODOLOGÍA

2.1 Descripción de la metodología

2.1.1 Unidad de análisis

Se reconoció como unidad de análisis a las tecnologías de información y comunicación de la compañía Corporación Impactex Cía. Ltda. ubicada en la calle 22 de enero y Circunvalación, vía Atahualpa junto al Complejo Revolition en el cantón Ambato provincia Tungurahua, dedicada se dedica a la producción de textiles. Además, de la comercialización, distribución, importación de otras marcas, y a partir de mayo 2020 empieza con la producción y distribución de prendas de bioseguridad.

2.1.2 Fuentes y técnicas de recolección de información

Fuentes de información primaria.- Para el desarrollo del proyecto integrador se obtuvo información de forma directa con los trabajadores de la compañía Corporación Impactex Cia. Ltda.

Tabla 5. Personas entrevistadas

Nombre	Cargo	Departamento
Josué Vélez	Ing., Informático	Sistemas
Cecibel Martínez	Auxiliar contable	Financiero
Juan Fernando Molina	Jefe de Área	Marketing
Andrés López	Ing. Informático	Sistemas

Elaborado por: Layedra (2022)

Encuesta.- A través de esta técnica se pudo obtener datos mediante la aplicación de un cuestionario previamente diseñado, fue aplicado el 19 de mayo de forma presencial con el objetivo de evaluar los controles generales e interno de las TIC en la compañía.

Cuestionario.- Se utilizaron preguntas previamente adaptadas del cuestionario del informe COSO 2013 y los 17 principios del mismo, este cuestionario está compuesta por preguntas cerradas con una escala nominal, como se presenta en la tabla 6.

Tabla 6. Cuestionario COSO 2013

Preguntas	Escala
Ambiente de control Circunstancias y conductas encaminadas en el accionar de la compañía desde el punto vista del control interno.	
Principio 1. Demuestra compromiso con la integridad y los valores éticos	
¿La asignación de responsabilidad y el establecimiento de políticas, son la base para el seguimiento de las actividades en el uso de las tecnologías?	o Si o No o No aplica
Principio 2. Ejerce Responsabilidad de Supervisión	
¿Se evalúan periódicamente los conocimientos de los miembros la compañía sobre el uso de las TIC?	o Si o No o No aplica
Principio 3. La Gerencia Establece estructura, autoridad, y responsabilidad	
¿La estructura organizativa y funcional permite el cumplimiento de sus objetivos?	o Si o No o No aplica
Principio 4. La organización demuestra compromiso por reclutar y mantener colaboradores competentes.	
¿La empresa mantiene comunicación directa con los empleados enfatizando sus responsabilidades y lo que la dirección espera de ellos?	o Si o No o No aplica
Principio 5. Hace cumplir con la responsabilidad	
¿Se realiza un reconocimiento a los colaboradores que se destaquen en el cumplimiento de las normas éticas, así como en el desempeño esperado?	o Si o No o No aplica
Evaluación de riesgos El riesgo es la probabilidad de ocurrencia de un evento no esperado que podría afectar a la compañía y su entorno.	
Principio 6. La organización define objetivos claros y relevantes, que permiten la identificación y evaluación de riesgos asociados.	
¿La empresa ha definido procedimientos claves para la identificación de vulnerabilidades en sus activos de información?	o Si o No o No aplica
Principio 7. Se identifican y analizan los riesgos para el logro de los objetivos.	
¿Los directivos de la compañía identifican los riesgos que pueden afectar el logro de los objetivos institucionales, en base a los factores internos o externos?	o Si o No o No aplica
Principio 8. Se evalúa el riesgo de Fraude	
¿Se evalúa los riesgos por ataques cibernéticos?	o Si o No o No aplica
Principio 9. Se identifican y analizan cambios importantes que puedan impactar el Sistema de Control Interno	
¿Se realiza un seguimiento del impacto que podrían tener la materialización de los riesgos sobre los objetivos de la compañía?	o Si o No o No aplica
ACTIVIDADES DE CONTROL La máxima autoridad, servidores y servidoras encargados del control interno, acorde a sus competencias establecerán políticas y procedimientos para dirigir los riesgos en el logro de los objetivos de la compañía, proteger y conservar los activos e implantar los controles a los sistemas de información.	
Principio 10. Seleccionar y Desarrollar Actividades de Control	
¿Tienen manuales, instructivos o normas de forma escrita que regulen el desarrollo de las diferentes actividades de trabajo con el uso de las TIC?	o Si o No o No aplica

Principio 11. La organización selecciona y desarrolla controles generales sobre tecnología	
¿Se han implementado controles orientados sobre el desarrollo, compra y mantenimiento de programas e infraestructura de TI?	o Si o No o No aplica
Principio 12. Implementación de las actividades de control, por medio de políticas y procedimientos.	
¿Los responsables de cada departamento diseñan controles relacionados con planes y programas de la actividad que desarrolla?	o Si o No o No aplica
INFORMACIÓN Y COMUNICACIÓN La máxima autoridad y directivos de la compañía deben identificar, capturar y comunicar información pertinente. Con la oportunidad de facilitar a los servidores y servidoras cumplir sus actividades.	
Principio 13. Generar y utilizar información relevante y de calidad.	
¿La calidad y oportunidad de la información permite la toma de decisiones adecuada, tanto hacia la máxima autoridad como a los jefes de los departamentos?	o Si o No o No aplica
Principio 14. Información Interna	
¿ La compañía ha definido los métodos de comunicación que son válidos en cada uno de los procesos, tales como correos electrónicos, memorandos internos, comités, intranet y mensajes de texto, entre otros?	o Si o No o No aplica
Principio 15. Comunicación Externa o a terceros	
¿Se han definido los responsables de la recepción de información de los entes externos, reduciendo la posibilidad de no atender un requerimiento por falta de gestión o conocimiento al interior de la organización?	o Si o No o No aplica
SEGUIMIENTO Y MONITOREO La máxima autoridad y directivos de la compañía establecerán procedimientos de seguimiento continuo, evaluaciones periódicas o la combinación de las dos para el aseguramiento de la eficacia del sistema de control interno de las TIC.	
Principio 16. Evaluaciones Continuas o Independientes	
¿Existen procedimientos para que la dirección revise los procesos de control de las TIC, para asegurarse de su cumplimiento del modo esperado?	o Si o No o No aplica
Principio 17. Evaluación y comunicación de las deficiencias encontradas.	
¿Los resultados de las evaluaciones realizadas, bien sea independientes o continuas son revisadas por los directivos o la Gerencia?	o Si o No o No aplica

Fuente: López Jara et al. (2018)

Elaborado por: Layedra (2022)

Entrevista.- Esta técnica se aplicó el 14 de abril del presente año, la mima que incluía una serie de preguntas siendo el apoyo para establecer ¿Cuáles eran las áreas en las que se debía aplicar una mejora?, se llevó a cabo de manera presencial con un representante del departamento de sistemas de la empresa.

Guion de entrevista.- El presente instrumento aplicado estaba compuesto por 40 preguntas, con una duración de 20 a 25 minutos, especificadas a manera de resumen en la tabla 6.

Tabla 7. Preguntas de la entrevista (visita preliminar)

¿La empresa ha tenido una auditoría informática en los años anteriores?
__Si __No
¿La empresa cuenta con un inventario de todos los equipos informáticos que posee?
__Si __No
¿El departamento de sistemas cuenta con un administrador de red informático?
__Si __No
¿Utilizan dispositivos especializados para las conexiones del exterior?
__Si __No
¿Se realiza mantenimiento a los activos de información?
__Si __No
¿Se analizan aplicaciones instaladas?
__Si __No
En caso de responder Si, contestar la siguiente pregunta
¿Con que frecuencia se realiza el análisis?
__Diariamente
__Una vez a la semana
__cada 15 días
__Una vez al año
¿Se evalúan técnicas y comportamiento del sistema?
__Si __No
¿Recibe bonificaciones por buen desempeño?
__Si __No
¿Los procedimientos están encaminados al cumplimiento de leyes, normas y reglamentos frente a las autoridades competentes?
__Si __No
Tiene recomendaciones para mejorar la gestión de las tecnologías de la información
_____ _____
¿Según su criterio cual es el área que presenta mayor riesgo dentro del departamento de sistemas?
_____ _____
Nombre del encuestado _____
Cargo_____

Elaborado por: Layedra (2022)

Revisión documental.- Esta técnica se aplicó de forma presencial y a través de medios digitales, con el objetivo de revisar información sobre el negocio (misión, visión, objetivos y procesos críticos), activos primarios y de soporte, seguridad de la información (confidencialidad, integridad, disponibilidad), riesgos (vulnerabilidades, amenazas, probabilidad de impacto), controles (administrativos, técnicos, físicos, legales), normativas (políticas, estándares, mejores prácticas), para el desarrollo de la auditoria. La solicitud de información se llevó a cabo a partir del 3 de mayo hasta el 20 del mismo mes.

Solicitud de requerimiento de información.- Gracias a este instrumento se solicitó una serie de requerimientos con el fin de dar inicio a la auditoria, como se detalla en la tabla 8.

Tabla 8. Requerimiento de información

Organigrama institucional
Misión, Visión y objetivos institucionales /estratégicos
Mapeo de los Sistemas de Información
Arquitectura de las conexiones de red
Inventario de activos de información y comunicación
Políticas internas
Normativa legal a la que se rige la compañía

Elaborado por: Layedra (2022)

2.1.3 Procesamiento de la información

Para el desarrollo del proyecto se ejecutó las fases de la auditoria, logrando el cumplimiento de los objetivos propuestos. Como se muestra en la tabla 9.

Tabla 9. Procesamiento de la información por objetivos

Objetivos	Técnica	Instrumento	Procedimiento	Producto
Elaborar la planificación de la auditoría informática para la evaluación de controles de las TIC, optimizando los recursos.	**Revisión documental** Con esta técnica se hizo una visita preliminar a la empresa dando una idea general del contexto normativo y tecnológico, procesos y tiempo a empleado. **Entrevista.** Dirigida a los que conforman el departamento de informática, y tener una visión global para ser sustento de la información recabada durante la observación.	Solicitud de requerimiento de información Guion de entrevista	**1. Fase de planificación y preparación** 1.1. Planeación estratégica -Guía de visita previa -Memorando 1.2. Planeación especifica -Entrevista	➢ Archivo permanente ➢ Programa de auditoria
Ejecutar la auditoría informática con la aplicación de programas y papeles de trabajo para la obtención de evidencias que permitan la sustentación de resultados.	**Encuesta.** es la recolección de información a través de un escrito, gráficos, etc. **Revisión documental**	Cuestionario Ficha de revisión (manuales, artículos)	**1. Fase 2 Ejecución** -Cuestionario en base a los 17 principios de la metodología COSO 2013. (dpto. Marketing, Sistemas y Finanzas) -Verificar las pruebas de cumplimiento y sustantivas	➢ Matriz de riesgo ➢ Enfoque de Auditoría ➢ Papeles de trabajo

	Observación directa		-Identificación de riesgos -Identificación de vulnerabilidades, amenazas susceptibles el área informática, activos, seguridad y sistemas de información.	➢ Hoja de hallazgos
Comunicar a través de la emisión del informe de auditoría informática las conclusiones y recomendaciones con respecto a los controles de las TIC.	**Confirmación y Verificación escrita.** Con esta técnica se comunicará a través de la redacción de los hechos obtenidos (hallazgos), con ello se verificará el cumplimiento de los procesos en el departamento de sistemas	Papeles de trabajo Hoja de Hallazgos	**2. Fase 3. Comunicación de resultados** Emitir la opinión con la descripción de los hechos encontrados con el apoyo de recomendaciones y conclusiones.	➢ Informe de auditoría de sistemas

Elaborado por: Layedra (2022)

Para el cumplimiento de los objetivos del presente proyecto se utilizó en su mayoría fuentes de recolección primarias, como lo define Cerda (1998) citado por Bernal Torres (2010) las fuentes primarias son de las cuales se consigue información directa, esto es, obtener información desde el lugar donde inicia los hechos, estas fuente pueden ser personas, empresas, acontecimientos, etc.

En el primer objetivo: Elaborar la planificación de la auditoría informática para la evaluación de controles de las TIC, optimizando los recursos. Se utilizó la técnica de revisión documental, con esta técnica se realizó una visita preliminar a la empresa generando una idea general del contexto normativo, tecnológico, factores externos y procesos, así determinar el tiempo a emplear, con la aplicación del instrumento de requerimiento de información. Además, se aplicó la técnica de entrevista a través de un guion de entrevista dirigida a quienes conforman el departamento de informática.

Todos estos instrumentos fueron aplicados para ser sustento de la información recabada durante el análisis de información y obtener el despliegue de procedimientos en la fase de planificación y preparación, tanto en la planeación estratégica como en la planificación específica, obteniendo como resultado el archivo permanente y el programa de auditoria

Para el segundo objetivo: Ejecutar la auditoría informática con la aplicación de programas y papeles de trabajo para la obtención de evidencias que permitan la sustentación de resultados, se empleó la técnica de encuesta que es la recolección de información a través de un escrito, gráficos, etc.

De este modo se empleó el instrumento del cuestionario según el marco de referencia COSO 2013 por cada componente, presentados en la tabla 10.

Tabla 10. Componentes COSO 2013

Ambiente de control	➢ Integridad ➢ Valores éticos ➢ Estructura organizativa, ➢ Responsabilidades

Evaluación de riesgos	➢ Identificación, respuesta y análisis de riesgos. ➢ Niveles aceptables sobre los riesgos
Actividades de control	➢ Controles conforme a las políticas y procedimientos.
Información y comunicación	➢ Calidad de información ➢ Impacto de mecanismos de protección de la información.
Monitoreo	➢ Evaluaciones continuas ➢ Apoyo externo ➢ Relevancia del uso de tecnologías

Elaborado por: Layedra (2022)

Todos los componentes redactados en la tabla 9 están orientados con base en los 17 principios COSO, que establecen un sistema de control interno que pueden ser aprovechados en toda la organización. Además, se aplicó pruebas de cumplimiento y sustantivas para la identificación de riesgos y vulnerabilidades a través de una matriz de riesgos, teniendo como producto los papeles de trabajo y la hoja de hallazgos.

En el tercer objetivo: Comunicar a través de la emisión del informe de auditoría informática las conclusiones y recomendaciones con respecto a los controles de las TIC con los hallazgos encontrados en la fase de ejecución, para que la institución implemente mejores prácticas en la confirmación y verificación del cumplimiento de los procesos en el departamento de sistemas.

Con el soporte de instrumentos como los papeles de trabajo y hoja de hallazgo que se desarrollaron con anterioridad en el proceso de la ejecución de la auditoria, en consecuencia, la obtención del Informe final.

CAPÍTULO III

DESARROLLO

3 Procesamiento de la información

Se realizó la auditoria Informática a la compañía Corporación Impactex Cía. Ltda. de la ciudad de Ambato para la verificación del cumplimiento de controles en la TIC como se presenta a continuación en cada una de las fases.

3.1 Fase I

PLANIFICACIÓN Y PREPARACIÓN

En esta primera fase se dio inicio a la planeación con una visita preliminar a la empresa Corporación Impactex Cia. Ltda. a esto se suma la realización de un archivo permanente que se adjuntó a los anexos de este proyecto integrador, como evidencia del cumplimiento de lo establecido en la guia de visita previa. Como resultado de lo anterior mencionado se desarrolló el programa de auditoria que fue la base de inicio de la segunda fase - ejecución.

3.1.1 Guia de visita previa

GUÍA DE VISITA PREVIA

GVP

1. INFORMACIÓN GENERAL	
1.1. Nombre de la entidad a Auditar	Corporación Impactex Cia. Ltda.
1.2. Número de Ruc	1891755755001
1.3. Dirección	Av. 22 de Enero y Circunvalación -ATAHUALPA
1.4. Correo electrónico de la empresa	impactex@hotmail.com sofynar1234@yahoo.es
1.5. Fecha de la visita	14 de febrero de 2022
1.6. Responsable de contestar la entrevista:	Ing. Josué Vélez – Dpto. de Sistemas
1.7. Entrevistador:	Soraya Belén Layedra Lagua – Auditor Senior

2. INFORMACIÓN AMBIENTE INTERNO			
PREGUNTA	**SI**	**NO**	**OBSERVACIÓN**
1. ¿Cuenta la empresa con misión?	x		Véase en APIG 2
2. ¿Cuenta la empresa con visión?	x		Véase en APIG 2
3. ¿Cuenta la empresa con una reseña histórica?	x		Véase en APIG 3
4. ¿Con qué objeto empresarial fue creada su empresa?	x		Véase en APIG 1
5. ¿La empresa cuenta con políticas?	x		Véase en APIG 2
6. ¿Cuenta la empresa con organigrama estructural en el que se muestre los departamentos en uso?	x		Véase en APIG 5
7. ¿Con cuántos empleados cuenta la empresa?	x		Véase en APIG6
8. ¿Cuenta con un Software Contable la empresa?	x		Véase en APIC 1
9. ¿Cuáles son los reportes que genera el sistema contable?	x		Véase en APIC 1
10. ¿Cuenta la empresa con asesoría para el mantenimiento de los equipos, de ser así, ¿cuál es el encargado?			Véase en APIC 2
11. ¿Cuáles son los activos de información con los que cuenta la empresa?	x		Véase en APIC 2
12. ¿Cuenta la empresa con productos estrella?	x		Véase en APIP 3
13. ¿Cuenta la empresa con condiciones de venta?	x		Véase en APIP 3
14. ¿Su empresa ha tenido anteriormente una Auditoria Informática?		x	No ha realizado Auditorias previas

Ing. Betancourt Kleber
Gerente General
Corporación Impactex Cia. Ltda.

Lcda. Belén Layedra
Auditor externo

3.1.2 Memorándum

MEMORANDO DE PLANIFICACIÓN PERIODO DEL 01 DE ENERO AL 31 DE DICIEMBRE DEL 2021	
Entidad :	Corporación Impactex Cia. Ltda.
Auditoria:	Auditoría Informática
Periodo:	2021
1. REQUERIMIENTO DE LA AUDITORIA	
Informe de Auditoría Informática	
2. FECHA DE INTERVENCIÓN	**Fecha estimada**
Planificación preliminar	Del 14-04-2022 hasta 29-04-2022
Planificación especifica	Del 01-05-2022 hasta 27-05-2022
Ejecución de la Auditoría	Del 30-05-2022 hasta 24-06-2022
Presentación del informe	Del 27-06-2022 hasta 29-07-2022

3. EQUIPO MULTIDISCIPLINARIO		
CARGO	**NOMBRE**	**INICIALES**
Jefe	Jiménez Estrella Patricia Paola	JEPP
Senior	Layedra Lagua Soraya Belén	LLSB

4. RECURSOS

Institucionales:	**Humanos:**	**Materiales:**
Universidad técnica de Ambato	Tutor de trabajo de titulación	Bibliografía
Facultad de contabilidad y Auditoría	Investigador – Investigadora	Software
Corporación Impactex Cia. Ltda.	Personal auxiliar	Hardware
	Asesores externos	
	Directivos del departamento de sistemas	

Económico:

Transporte	$	96,00	
Imprevistos	$	30,00	
Bibliografía	$	35,00	
Papelería	$	50,00	
Total	$	211,00	**Dólares**

5. ENFOQUE DE LA AUDITORIA

5.1 Información general de la entidad auditada

-Misión

Somos una organización dedicada a la Innovación desarrollo y comercialización de marcas de moda con excelencia posicionándonos en los mercados nacionales y extranjeros para generar rentabilidad, sostenibilidad y crecimiento empresarial para nuestros clientes internos y externos.

-Visión

Ser un grupo empresarial líder en el mercado de moda con excelencia, responsabilidad social, empresarial y ambiental, internacionalizando nuestras marcas para crecer y consolidarnos, con nuestros consumidores neo tradicionales casuales.

-Objetivo

OBJETIVO ESTRATÉGICO

Generar recursos económicos por medio del desarrollo y la comercialización del portafolio de productos de Marcas, para satisfacer necesidades de vestimenta y estilo neo tradicional del mercado nacional e internacional.

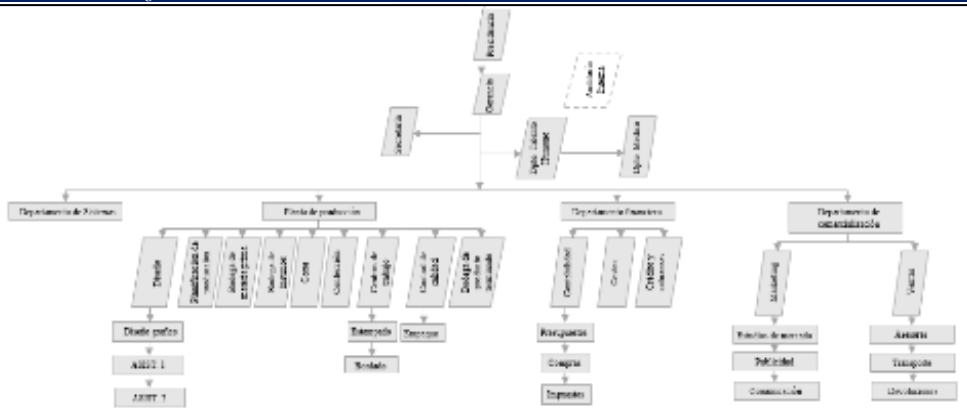
POLÍTICA DE CALIDAD

Quienes integramos el GRUPO IMPACTEX estamos comprometidos a elaborar productos acorde a la moda innovando y diseñando prendas de calidad para cumplir las necesidades de nuestros clientes

-Actividades Principales

Producto:
Ropa interior femenina y masculina
Ropa deportiva
Prendas de bioseguridad

-Estructura orgánica



- Base Legal

Constitución del Ecuador
Ley de Régimen Tributario Interno
Reglamento para la aplicación de la Ley de régimen tributario Interno
Código de Trabajo
Ley de la Propiedad Intelectual
Supervisado por la Superintendencia de Compañías

SUPERINTENDENCIA DE COMPAÑÍAS

EXTRACTO

CONSTITUCIÓN DE LA COMPAÑÍA **CORPORACIÓN IMPACTEX CÍA. LTDA..**

La compañía **CORPORACIÓN IMPACTEX CÍA. LTDA.** se constituyó por escritura pública otorgada ante el Notario Segundo Encargado del **Cantón AMBATO, el 13/01/2014**, fue aprobada por la Superintendencia de Compañías, mediante Resolución SC.DIC.A.14. 067

1.- DOMICILIO: Cantón AMBATO, provincia de TUNGURAHUA.

2.- CAPITAL:Suscrito US$ 400,00 Número de Participaciones 400 Valor US$ 1,00

3.- OBJETO: El objeto de la compañía es: "..PRODUCCIÓN, ELABORACIÓN, TERMINADO, COMERCIALIZACIÓN, DISTRIBUCIÓN, IMPORTACIÓN, EXPORTACIÓN DE TODO TIPO DE TEXTILES Y PRENDAS DE VESTIR..."

Ambato, 11 FEB. 2014

5.2 Motivo de la auditoría

La Auditoría Informática que se realizó a la compañía Corporación Impactex Cia. Ltda. Tuvo el fin de evaluar los principales controles del uso de las TIC y de la correcta gestión de los mismos.

5.3 Enfoque a:

La auditoría informática tiene el fin de mejorar y elevar el valor de la compañía CORPORACIÓN IMPACTEX Cia. Ltda. proporcionando aseguramiento y análisis sobre los posibles riesgos, principios de integridad, competencia y diligencia profesional que beneficia la evaluación, seguimiento y monitoreo en la gestión de tecnologías y de un adecuado uso de las TIC para la detección de riesgos y aplicación de controles.

5.4. Objetivos

Objetivo General

Ejecutar la auditoría informática a la Empresa Corporación Impactex Cía. Ltda. de la ciudad de Ambato para la verificación del cumplimiento de controles de las TIC.

Objetivos Específicos

Ø Elaborar la planificación de la auditoría informática para la evaluación de controles de las TIC.

Ø Ejecutar la auditoría informática con la aplicación de programas y papeles de trabajo para la obtención de evidencias que permitan la sustentación de resultados.

Ø Comunicar a través de la emisión del informe de auditoría informática las conclusiones y recomendaciones con respecto a los controles de las TIC.

5.5. Alcance

Se realizará una Auditoría Informática a la empresa Corporación Impactex Cia. Ltda. del periodo 2021, a través de la aplicación de un cuestionario direccionado a los 17 principios del marco COSO 2013, determinando deficiencias tanto en la gestión de las TI como en los Activos de información y seguridad de la información. Así mismo, el análisis de los aspectos positivos y negativos desde la instalación de nuevas tecnologías, contratación de personal, desarrollo de software, comprobación y el estado de instalaciones para garantizar la seguridad, periodicidad de controles y monitoreo de los mismos.

5.6. Resumen de los Resultados de la Evaluación preliminar

En el control interno, en cuanto a la segregación de funciones específicas, asignación de claves, periodicidad de mantenimientos lógicos y control de los activos de información.

En el Sistema de gestión de la seguridad de la información (SGSI) se limitan en la aplicación de los estándares de la norma ISO 27000. Están sujetos a políticas internas impuestas por la empresa.

Presentan un control mínimo en la comprobación, integridad y autenticidad de seguridad de datos.

Escasa aplicación de políticas de restricción en el uso de equipos informáticos.

Aplican controles medios en la seguridad de información, por lo tanto, reduce la prevención de riesgos.

6 TRABAJO A REALIZAR EN LA FASE DE EJECUCIÓN

6.1 TRABAJO A REALIZAR POR LOS AUDITORES EN LA FASE DE EJECUCIÓN

Objetivo	Técnica	Instrumento	Procedimiento	Producto
Ejecutar la auditoría informática con la aplicación de programas y papeles de trabajo para la obtención de evidencias que permitan la sustentación de resultados.	**Encuesta.** es la recolección de información a través de un escrito, gráficos, etc. **Revisión documental** Con esta técnica se hará una visita preliminar a la empresa en la que generará una idea general del contexto normativo y tecnológico, factores externos, procesos y determinar el tiempo a emplear	Cuestionario	-Cuestionario en base a los 17 principios de la metodología COSO 2013. -Efectuar pruebas de cumplimiento y sustantivas -Identificación de riesgos	Ø Matriz de riesgo Ø Papeles de trabajo Ø Hoja de hallazgos

7. COLABORACIÓN DE LA ENTIDAD AUDITADA

7.1 Auditores internos

NO APLICA

7.2 Otros profesionales

Nombre	Cargo	Departamento
Josué Vélez	Ing., Informático	Sistemas
Cecibel Martínez	Auxiliar contable	Financiero
Juan Fernando Molina	Jefe de Área	Marketing
Andrés López	Ing. Informático	Sistemas

8. OTROS ASPECTOS

Se desarrolló el archivo permanente como
soporte del presente memorándum
Se levantó un inventarios de los activos de información tanto físicos como lógicos de la empresa Corporación Impactex Cia. Ltda.
Se anexó los papeles de trabajo utilizados para el desarrollo de la fase de la ejecución de la auditoria

9. FIRMAS DE RESPONSABILIDAD

9.1 Elaborado por

Layedra Lagua Soraya Belén

Auditor Senior

Fecha:
8/06/2022

9.2 Validado por

Jiménez Estrella Patricia Paola

Auditor Jefe

Fecha:
8/06/2022

Elaborado por:	**LLSB**
Fecha:	8/6/2022
Revisado por:	**JEPP**
Fecha:	9/6/2022

3.1.3 Programa de auditoría

PA

Corporación Impactex Cia. Ltda.
PROGRAMA DE AUDITORÍA
COMPONENTES: Gestión de las tecnologías
Activos de Información
Seguridad de la Información
AÑO 2021

OBJETIVOS

1. Evaluar el control interno en la gestión de las tecnologías, activos de información y seguridad de la información
2. Determinar los riesgos relevantes en la seguridad del uso de las TIC de la compañía
3. Determinar la magnitud de los riesgos encontrados

N.	PROCEDIMIENTOS	REF - PT	ELABORADO POR	FECHA
Procedimiento sustantivo				
1.	Aplicar el cuestionario COSO en diferentes departamentos	CC	SBLL	13/6/2022
2.	Seleccionar los riesgos más relevantes	CC	SBLL	14/6/2022
3.	Determinar el nivel de confianza y el nivel de riesgo	NC - NR	SBLL	15/6/2022
4.	Establecer el enfoque de auditoría	ER	SBLL	16/6/2022
5.	Tomar los resultados de la aplicación del cuestionario y elaborar la matriz de riesgo	MR	SBLL	17/6/2022
Procedimientos Generales				
1.	Ejecutar el cuestionario de la metodología COSO 2013			
2.	Desarrollar la matriz de riesgos			
3.	Elaborar el mapa de calor			
4.	Redactar la hoja de hallazgos			

Elaborado por:	**LLSB**
Fecha:	8/6/2022
Revisado por:	**JEPP**
Fecha:	9/6/2022

3.2 Fase II

EJECUCIÓN

3.2.1 Evaluación especifica de la estructura de control interno

A continuación, se presenta un resumen resultado de la aplicación del cuestionario COSO 2013 hacia los diferentes departamentos de la compañía, donde se determinó nivel de riesgo través de la semaforización como se detalla en la tabla 11.

Tabla 11. Ponderación del nivel de confianza y nivel de riesgo

NIVEL DE CONFIANZA		
BAJO	**MODERADO**	**ALTO**
5%-50%	51% - 75%	76% - 95%
95%-50%	49% - 25%	24% - 5%
ALTO	**MODERADO**	**BAJO**
NIVEL DE RIESGO (100-NC)		

CC-1

Corporación Impactex Cia. Ltda.
Evaluación específica de la estructura de control interno
Componente: Controles del uso de las TIC
Del 1 de enero al 31 de diciembre del 2021

CUESTIONARIO DE CONTROL INTERNO
Departamento de Finanzas

NIVEL DE CONFIANZA GENERAL

VALORACIÓN $NC=\frac{CT}{PT}x100$		
Calificación Total	(C.T.) =	41
Ponderación Total	(P.T.) =	49
Nivel de Confianza	NC= CT/PT x 100	83,67%
Nivel de Riesgo Inherente / De control	RI-RC= 100% - NC%	16,33%
		BAJO

Elaborado por:	**LLSB**
Fecha:	8/6/2022
Revisado por:	**JEPP**
Fecha:	9/6/2022

MR-1

Corporación Impactex Cia. Ltda.
MAPEO DE RIESGO
PERÍODO: AÑO 2021
Departamento de Finanzas

MAPA DE RIESGO			RIESGO	ENFOQUE
AMBIENTE DE CONTROL			*MODERADO*	MIXTO-DOBLE PROPÓSITO
CT	10	NC - RI	ARGUMENTO PARA EL RIESGO	
PT	14		No se evalúan periódicamente los conocimientos de los miembros la compañía sobre el uso de las TIC. No se socializa el plan de capacitación al personal de la compañía.	
NC	71%	*MODERADO*		
RI	29%	*MODERADO*		

MAPA DE RIESGO			RIESGO	ENFOQUE
EVALUACIÓN DE RIESGOS			*BAJO*	CUMPLIMIENTO
CT	9	NC - RI	ARGUMENTO PARA EL RIESGO	
PT	11		No se realiza un seguimiento del impacto que podrían tener la materialización de los riesgos sobre los objetivos de la compañía.	
NC	82%	*ALTO*		
RI	18%	*BAJO*		

MAPA DE RIESGO			RIESGO	ENFOQUE
ACTIVIDADES DE CONTROL			*BAJO*	CUMPLIMIENTO
CT	30	NC - RI	ARGUMENTO PARA EL RIESGO	
PT	35		N/A	
NC	86%	*ALTO*		
RI	14%	*BAJO*		

MAPA DE RIESGO			RIESGO	ENFOQUE
INFORMACIÓN Y COMUNICACIÓN			*BAJO*	CUMPLIMIENTO
CT	7	NC - RI	ARGUMENTO PARA EL RIESGO	
PT	8		No se realizan acciones de seguimiento, que permitan validar el cumplimiento de los objetivos de la organización.	
NC	88%	*ALTO*		
RI	13%	*BAJO*		

MAPA DE RIESGO			RIESGO	ENFOQUE
SEGUIMIENTO Y MONITOREO			*BAJO*	CUMPLIMIENTO
CT	4	NC - RI	ARGUMENTO PARA EL RIESGO	
PT	5		No existen procedimientos para que la dirección revise los procesos de control de las TIC, para asegurarse de su cumplimiento del modo esperado.	
NC	80%	*ALTO*		
RI	20%	*BAJO*		

RESUMEN DEL MAPEO DE RIESGOS			
COMPONENTE	**NIVEL DE CONFIANZA**	**NIVEL DE RIESGO**	**SEMAFORIZACIÓN DEL NIVEL DE CONFIANZA**
Ambiente de control	71%	29%	***MODERADO***
Evaluación de riesgo	82%	18%	***BAJO***
Actividades de Control	86%	14%	***BAJO***
Información y Comunicación	88%	13%	***BAJO***
Seguimiento y Monitoreo	80%	20%	***BAJO***

Elaborado por:	**LLSB**
Fecha:	8/6/2022
Revisado por:	**JEPP**
Fecha:	9/6/2022

CC-2

Corporación Impactex Cia. Ltda.
Evaluación específica de la estructura de control interno
Componente: Controles del uso de las TIC
Del 1 de enero al 31 de diciembre del 2021

CUESTIONARIO DE CONTROL INTERNO
Departamento de Marketing

NIVEL DE CONFIANZA GENERAL

VALORACIÓN

NC= $\frac{CT}{PT} x100$

Calificación Total	(C.T.)=	45
Ponderación Total	(P.T.)=	51
Nivel de Confianza	NC= CT/PT x 100	88,24%
Nivel de Riesgo Inherente / De control	RI-RC= 100% - NC%	11,76%
	BAJO	

Elaborado por:	**LLSB**
Fecha:	8/6/2022
Revisado por:	**JEPP**
Fecha:	9/6/2022

MR-2

Corporación Impactex Cia. Ltda.
MAPEO DE RIESGO
PERÍODO: AÑO 2021
Departamento de Marketing

MAPA DE RIESGO			RIESGO	ENFOQUE
AMBIENTE DE CONTROL			*MODERADO*	MIXTO-DOBLE PROPÓSITO
CT	11	NC - RI	ARGUMENTO PARA EL RIESGO	
PT	16		No se evalúan periódicamente los conocimientos de los miembros la compañía sobre el uso de las TIC. La empresa no mantiene comunicación directa con los empleados enfatizando sus responsabilidades y lo que la dirección espera de ellos. No se socializa el plan de capacitación al personal de la compañía.	
NC	69%	*MODERADO*		
RI	31%	*MODERADO*		

MAPA DE RIESGO			RIESGO	ENFOQUE
EVALUACIÓN DE RIESGOS			*BAJO*	CUMPLIMIENTO
CT	9	NC - RI	ARGUMENTO PARA EL RIESGO	
PT	10		No se ha definido procedimientos claves para la identificación de vulnerabilidades en sus activos de información.	
NC	90%	*ALTO*		
RI	10%	*BAJO*		

MAPA DE RIESGO			RIESGO	ENFOQUE
ACTIVIDADES DE CONTROL			*BAJO*	CUMPLIMIENTO
CT	30	NC - RI	ARGUMENTO PARA EL RIESGO	
PT	35		N/A	
NC	86%	*ALTO*		
RI	14%	*BAJO*		

MAPA DE RIESGO			RIESGO	ENFOQUE
INFORMACIÓN Y COMUNICACIÓN			*BAJO*	CUMPLIMIENTO
CT	8	NC - RI	ARGUMENTO PARA EL RIESGO	
PT	8		N/A	
NC	100%	*ALTO*		
RI	0%	*BAJO*		

MAPA DE RIESGO			RIESGO	ENFOQUE
SEGUIMIENTO Y MONITOREO			*BAJO*	CUMPLIMIENTO
CT	5	NC - RI	ARGUMENTO PARA EL RIESGO	
PT	5		N/A	
NC	100%	*ALTO*		
RI	0%	*BAJO*		

RESUMEN DEL MAPEO DE RIESGOS			
COMPONENTE	**NIVEL DE CONFIANZA**	**NIVEL DE RIESGO**	**SEMAFORIZACIÓN DEL NIVEL DE CONFIANZA**
Ambiente de control	69%	31%	***MODERADO***
Evaluación de riesgo	90%	10%	***BAJO***
Actividades de Control	86%	14%	***BAJO***
Información y Comunicación	100%	0%	***BAJO***
Seguimiento y Monitoreo	100%	0%	***BAJO***

Elaborado por:	**LLSB**
Fecha:	8/6/2022
Revisado por:	**JEPP**
Fecha:	9/6/2022

CC-3

Corporación Impactex Cia. Ltda.
Evaluación específica de la estructura de control interno
Componente: Controles del uso de las TIC
Del 1 de enero al 31 de diciembre del 2021

CUESTIONARIO DE CONTROL INTERNO
Departamento de Sistemas

NIVEL DE CONFIANZA GENERAL

VALORACIÓN

NC= $\frac{CT}{PT} x100$

Calificación Total	(C.T.)=	51
Ponderación Total	(P.T.)=	53
Nivel de Confianza	NC= CT/PT x 100	96,23%
Nivel de Riesgo Inherente / De control	RI-RC= 100% - NC%	3,77%
	BAJO	

Elaborado por:	**LLSB**
Fecha:	8/6/2022
Revisado por:	**JEPP**
Fecha:	9/6/2022

MR-3

Corporación Impactex Cia. Ltda.
MAPEO DE RIESGO
PERÍODO: AÑO 2021
Departamento de Sistemas

MAPA DE RIESGO			RIESGO	ENFOQUE
AMBIENTE DE CONTROL			***BAJO***	CUMPLIMIENTO
CT	**15**	**NC - RI**	**ARGUMENTO PARA EL RIESGO**	
PT	16		Se modifica de forma constante la estructura, funciones y responsabilidades en la compañía.	
NC	94%	***ALTO***		
RI	6%	***BAJO***		

MAPA DE RIESGO			RIESGO	ENFOQUE
EVALUACIÓN DE RIESGOS			*BAJO*	CUMPLIMIENTO
CT	11	NC - RI	ARGUMENTO PARA EL RIESGO	
PT	12		No se realiza un seguimiento del impacto que podrían tener la materialización de los riesgos sobre los objetivos de la compañía	
NC	92%	*ALTO*		
RI	8%	*BAJO*		
MAPA DE RIESGO			RIESGO	ENFOQUE
ACTIVIDADES DE CONTROL			*BAJO*	CUMPLIMIENTO
CT	30	NC - RI	ARGUMENTO PARA EL RIESGO	
PT	35		N/A	
NC	86%	*ALTO*		
RI	14%	*BAJO*		

MAPA DE RIESGO			RIESGO	ENFOQUE
INFORMACIÓN Y COMUNICACIÓN			*BAJO*	CUMPLIMIENTO
CT	8	NC - RI	ARGUMENTO PARA EL RIESGO	
PT	8		N/A	
NC	100%	*ALTO*		
RI	0%	*BAJO*		

MAPA DE RIESGO			RIESGO	ENFOQUE
SEGUIMIENTO Y MONITOREO			*BAJO*	CUMPLIMIENTO
CT	5	NC - RI	ARGUMENTO PARA EL RIESGO	
PT	5		N/A	
NC	100%	*ALTO*		
RI	0%	*BAJO*		

RESUMEN DEL MAPEO DE RIESGOS			
COMPONENTE	NIVEL DE CONFIANZA	NIVEL DE RIESGO	SEMAFORIZACIÓN DEL NIVEL DE CONFIANZA
Ambiente de control	94%	6%	*BAJO*
Evaluación de riesgo	92%	8%	*BAJO*
Actividades de Control	86%	14%	*BAJO*
Información y Comunicación	100%	0%	*BAJO*
Seguimiento y Monitoreo	100%	0%	*BAJO*

Elaborado por:	**LLSB**
Fecha:	8/6/2022
Revisado por:	**JEPP**
Fecha:	9/6/2022

3.2.2 Activos de Información y riesgos asociados

Para la evaluación de los principales riesgos en el uso de activos de información con los que cuenta la compañía se determinó a través de una técnica visual conocida como mapa de calor. Con el uso de esta técnica se pudo visualizar de manera clara la probabilidad de los riesgos, escala que fue determinada por colores como se describe en la tabla 12.

Tabla 12. Administración de Riesgos

Escala de probabilidad		
Probabilidad	**Calificación cuantitativa**	**Calificación cualitativa**
Improbable	1	Puede ocurrir al menos una vez en periodos superiores a 5 años
Poco probable	2	Puede ocurrir al menos una vez entre 1 y 5 años
Probable	3	Puede ocurrir al menos una vez al año
Muy probable	4	Puede ocurrir varias veces en un mes
Altamente probable	5	Puede ocurrir al menos una vez al día

Elaborado por: Layedra (2022)

Para la aplicación de esta evaluación se determinó las vulnerabilidades y amenazas de los activos de información de la compañía (tabla 13).

Tabla 13. Amenazas y vulnerabilidades de los activos de información

Activos de Información	Vulnerabilidad	Amenaza
Sistema contable Jireh e Incorp	Inadecuada implementación de mejoras	Interrupción de procesos de negocio.
29 Computadoras de escritorio	Inadecuada seguridad física, virus informáticos, Sensible a cambios de voltaje	Ocultar identificación de usuario
4 Computadoras portátil		Robos, robos de información
8 Impresoras multifuncionales pequeñas 3 Impresoras matriciales 1 Impresora Zebra 1 Impresora Xerox Altalink 1 Impresora RICO MP Proyector Cajón para dinero	Falta de mantenimiento	Golpes, desastres naturales, cortes eléctricos, robos, caídas y uso inadecuado.

Microsoft Office	Falta de un sistema de identificación y autenticidad de usuario, Incompatibilidad de formatos, falta de memoria para actualizaciones.	Acceso por usuarios no autorizados, perdida de información, códigos maliciosos, Lentitud en el sistema.
Páginas electrónicas de venta	Interfaz complicado para el cliente, control mínimo en los datos de entrada y salida, poca supervisión de los vendedores.	Malware dirigen a los usuarios a páginas falsas, eliminación de información del negocio, interrupciones en el servicio.
Correos electrónicos	Hackeo de cuentas, información falsa	Difusión de contraseñas, espionaje, compartir información confidencial.
Redes Sociales		
Discos externos de almacenamiento	Incompatibilidad con los ordenadores, perdida	Robo, destrucción.
Router	Sensible a cambios de voltaje, mínima seguridad de cableado.	Hackeo, daño eléctrico, desastre natural.
Cámaras de seguridad	Sensible a la temperatura, humedad, inadecuado control de acceso.	corte eléctrico, robo, deterioro, espionaje
Antivirus	Bloqueo del PC, ejecución de malware, códigos maliciosos.	Infección por dispositivos USB, spam, re direccionamiento de URL, fuga de información, gusano informático
Factor humano (directivos, jefes departamentales, asesores, operarios)	Segregación de funciones y responsabilidades, mínima supervisión a los empleados, información deficiente.	Paros, desastres naturales, utilización incorrecta de las TIC, personal infiltrado, fraude, divulgación de información.

Elaborado por: Layedra (2022)

3.2.2.1 Riesgo total

Para la determinación de los niveles de riesgo se tomó como referencia la escala de valores que van desde menos tres como un riesgo bajo hasta un valor mayor o igual a veinte, como se presenta en la tabla 14.

Tabla 14. Nivel del riesgo total

Nivel de riesgo	Valores
Bajo	<3
Moderado	>=3 y <5
Medio	>=5 y <10
Alto	>=10 y <20
Muy Alto	>=20

Elaborado por: Layedra (2022)

Una vez analizado la probabilidad y el impacto del riesgo se logró establecer el riesgo total como se especifica en la tabla 14.

Tabla 15. Nivel de riesgos

Activos de Información	Descripción del riesgo	Probabilidad	Impacto	Riesgo total
Sistema contable Jireh e Incorp	Riesgo en el sistema contable por las mejoras que se están aplicando para el año 2022.	2	4	8
29 Computadoras de escritorio	Perdida de información, equipos, daños, no se identifica acceso de usuario.	1	5	5
4 Computadoras portátil		1	5	5
8 Impresoras multifuncionales pequeñas 3 Impresoras matriciales 1 Impresora Zebra 1 Impresora Xerox Altalink 1 Impresora RICO MP Proyector Cajón para dinero	Fallos en los equipos, perdida, suspensión de actividades.	2	5	10
Microsoft Office	Divulgación de información, interrupción de tareas, ingreso de información no autorizada.	1	5	5
Páginas electrónicas de venta	Riesgo de fraude por información falsa.	1	4	4

Correos electrónicos	Recibir correos spam con enlaces maliciosos.	2	3	6
Redes Sociales	Compartir información errónea.	1	3	3
Discos externos de almacenamiento	Riesgo en la perdida de información por la falta de respaldos.	2	4	8
Router	No tener internet necesario para el desarrollo de algunas actividades de la compañía.	1	2	2
Cámaras de seguridad	Riesgo en la interrupción de su funcionamiento.	2	3	6
Antivirus	Robo de información, bloqueo de actividades, demora en el procesamiento de información.	2	4	8
Factor humano (directivos, jefes departamentales, asesores, operarios)	Incumplimiento de tareas, no se logra el cumplimiento de objetivos, falta del cumplimiento de controles.	4	5	20

Elaborado por: Layedra (2022)

3.2.2.2 Recomendaciones de los riesgos asociados

A partir del establecimiento del nivel de riesgo por parte de auditoria se determina recomendaciones con el objetivo de mitigar los riesgos detectados.

Tabla 16. Recomendaciones sobre los riesgos

Descripción del riesgo	Recomendación	Responsable del control	Frecuencia del control
Riesgo en el sistema contable por las mejoras que se están aplicando para el año 2022.	Supervisar los avances y resultados de las nuevas implementaciones	Jefe de sistemas	cada 15 días
Perdida de información, equipos, daños, no se identifica acceso de usuario.	Llevar un control de los inventarios a través de una matriz donde se especifique el estado y	Jefe de sistemas	mensual

	funcionamiento de los mismos		
Fallos en los equipos, perdida, suspensión de actividades.	Asignar un encargado de realizar el mantenimiento	Jefe de sistemas	mensual
Divulgación de información, interrupción de tareas, ingreso de información no autorizada.	Llevar el control de las actividades realizadas por cada usuario	Cada empleado	diario
Riesgo de fraude por información falsa.	Verificar la información recibida por los posibles clientes	Jefe de marketing	s/f
Recibir correos spam con enlaces maliciosos.	Evitar abrir correos spam y re direccionarse a los URL de los mismos	Todos los departamentos	diario
Compartir información errónea.	Verificar la información antes de publicarla	Dpto. de marketing	s/f
Riesgo en la perdida de información por la falta de respaldos.	Asignar un encargado de verificar que el disco duro este en buen estado y funcionamiento	Dpto. de sistemas	s/f
No tener internet necesario para el desarrollo de algunas actividades de la compañía.	Tener acceso a redes alternas	Dpto. de sistemas	s/f
Riesgo en la interrupción de su funcionamiento.	Asignar a un encargado de monitorear el correcto funcionamiento de las cámaras de seguridad	Jefe de sistemas	mensual
Robo de información, bloqueo de actividades, demora en el procesamiento de información.	Asignar un responsable de la actualización de antivirus y que verifique que tenga una buena protección	Jefe de sistemas	mensual
Incumplimiento de tareas, no se logra el cumplimiento de objetivos, falta del cumplimiento de controles.	Supervisar el cumplimiento de tareas por cada empleado de la compañía	Jefe de Talento Humano	mensual

Elaborado por: Layedra (2022)

3.2.2.2 Tratamiento de del riesgo

A continuación, se presenta la administración del riesgo con el fin de aplicar medidas correctivas adecuadas que sean de apoyo para que la organización tenga un control optimo sobre las TIC. Para mejor entendimiento de la Tabla 17 es importante conocer que un riesgo asumido es cuando la compañía asume el riesgo en su totalidad, el riesgo mitigado es cuando la empresa tiene la capacidad de limitar el impacto que puede tener la ocurrencia de un riesgo y el riesgo compartido es aquel en el que la compañía reduce el efecto o impacto al transferir a otra empresa.

Tabla 17. Administración del riesgo

Administración del riesgo	Descripción del riesgo
Asumido	Riesgo en el sistema contable por las mejoras que se están aplicando para el año 2022.
	Compartir información errónea.
	No tener internet necesario para el desarrollo de algunas actividades de la compañía.
	Riesgo en la interrupción de su funcionamiento.
	Robo de información, bloqueo de actividades, demora en el procesamiento de información.
Mitigado	Perdida de información, equipos, daños, no se identifica acceso de usuario
	Incumplimiento de tareas, no se logra el cumplimiento de objetivos, falta del cumplimiento de controles.
	Fallos en los equipos, perdida, suspensión de actividades.
	Recibir correos spam con enlaces maliciosos
	Riesgo en la perdida de información por la falta de respaldos.
	Divulgación de información, interrupción de tareas, ingreso de información no autorizada.
Compartido	Riesgo de fraude.

Elaborado por: Layedra (2022)

3.2.3 Hoja de hallazgos

El instrumento que se presenta a continuación, permitió la redacción clara de los hechos importantes encontrados durante la ejecución de la auditoria del periodo 2021, referente al uso adecuado de las TIC en Corporación Impactex Cia. Ltda.

HH

Corporación Impactex Cia. Ltda.					
HOJA DE HALLAZGOS					
COMPONENTE	**TITULO (RIESGOS)**	**REF. PT**	**ATRIBUTOS DEL HALLAZGO**	**COMENTARIOS**	**RECOMENDACIONES**
Diagnostico preliminar	1. Políticas del uso de equipos informáticos.	M	**CONDICIÓN**	Hay escasa aplicación de políticas de restricción en el uso de equipos informáticos.	Al dpto. de sistemas mantener los soportes informáticos en un lugar cerrado al momento en que no sean utilizados, además aplicar un control de bloqueo de pantallas y designación de contraseñas para proteger los equipos que se encuentran sin vigilancia.
			CRITERIO	Según la norma ISO 27001 controles de la seguridad de los equipos informáticos. Los quipos necesitan atención particular y estar protegidos ante amenazas externas con el fin de evitar el acceso no autorizado o inapropiado, también de robos o pérdidas considerables.	
			CAUSA	Tienen equipos aislados y están a libre uso de los trabajadores de la compañía.	
			EFECTO	Dificultad de identificar al usuario que le dio al uso al equipo informático en caso de pérdida o daño del mismo.	
	2. Aplicación de controles en la seguridad de información.	M	**CONDICIÓN**	Se aplica controles medios en la seguridad de información reduciendo la prevención de riesgos.	Al jefe de sistemas implementar una política sobre la seguridad de la información en la que se establezca los tipos de controles a aplicar tales como preventivos, detectivos y correctivos.
			CRITERIO	Según la norma ISO 27002 en todas las organizaciones se debe fijar una política sobre la seguridad de información, el mismo que contendrá la estructura, objetivos y la forma del control que tendría la información de la empresa.	
			CAUSA	No hay una cultura sobre la aplicación de controles eficientes y funcional, así como preventivos, correctivos o correctivos.	
			EFECTO	No se tiene la certeza de la efectividad del control ya que al aplicar un control medio no determina si la seguridad está bien o mal.	

Ambiente de Control	3. Evaluación periódica de los conocimientos de los miembros la compañía sobre el uso de las TIC.	MR-1 MR-2	**CONDICIÓN**	En el departamento de finanzas y marketing de la compañía tiene una débil evaluación periódica de los conocimientos de los miembros de la compañía sobre el uso de las TIC.	Al gerente de empresa Corporación Impactex Cia. Ltda. asignar personal para que se encargue de la evaluación periódica de los departamentos de marketing y financiero.
			CRITERIO	Según la norma ISO 9001: 2015 cláusula 7.1.6 el conocimiento organizacional es producto de la experiencia de cada individuo la misma que debe ser evaluada. De esta forma permitirá incorporar mejores conocimientos que serán aplicados en el desarrollo de procesos. Así mismo el mantenimiento, actualización y administración de la información es una vía que asegura la valides del conocimiento.	
			CAUSA	Falta de un colaborador encargado en la revisión por departamentos.	
			EFECTO	Tener trabajadores con bajo rendimiento.	
	4. Inasistencia a la capacitaciones socializadas según el plan de capacitación.	MR-1 MR-2	**CONDICIÓN**	El personal de los departamentos de finanzas y marketing de la compañía no asisten las capacitaciones planificadas.	Al departamento de Talento Humano elaborar un cronograma de capacitación para cada departamento con horarios dentro de la jornada laboral.
			CRITERIO	Según las NCI apartado 410-15 Capacitación informática. Las capacitaciones serán impartidas tanto para el personal de TI así también para los usuarios por ello deberán contar con un plan de capacitación desarrollado con el apoyo del departamento del talento humano. Tiene el fin de satisfacer las necesidades de conocimientos específicos.	
			CAUSA	Las capacitaciones son impartidas en horarios fuera de la jornada laboral	
			EFECTO	Desventaja de los trabajadores en actualización de temas en cuestión a nuevas tecnologías.	
	5. Comunicación directa con los empleados sobre sus responsabilidades y lo que la dirección espera de ellos.	MR-2	**CONDICIÓN**	En el departamento de marketing hay escasa comunicación directa con los empleados sobre sus responsabilidades y lo que la dirección espera de ellos	Al jefe de marketing preparar especificar las responsabilidad de cada empleado y los objetivos a alcanzar al momento de incorporar a un empleado en su departamento.
			CRITERIO	Según la norma ISO 9001: 2015 especifica los aspectos de comunicación tanto internos como externos que determinará la eficiencia de la organización, además, que se deben establecer canales de comunicación en el que se establezca el tiempo y el responsable de realizar la comunicación.	
			CAUSA	Se da una explicación general al momento de la contratación y no se realiza una retroalimentación sobre las responsabilidades que tiene cada empleado por parte del jefe del departamento.	
			EFECTO	Poca claridad en las actividades que deben realizar y por ende baja productividad para la compañía.	
	6. Estructura, funciones y	MR-3	**CONDICIÓN**	En el departamento de sistemas se modifican de forma constante su estructura, funciones y responsabilidades.	Al jefe del departamento de sistemas supervisar que el

	responsabilidades en el departamento.		**CRITERIO**	Según las NCI apartado 410-02. Segregación de funciones. Las funciones y responsabilidad deben ser definidos de forma clara y comunicados de manera formal que permitirá que los roles sean ejercidos con autoridad. Las responsabilidades pueden ser varias dentro de un mismo cargo.	personal a cargo realice las actividades según sus perfiles en cada una de sus tareas.
			CAUSA	No cumplimiento de las funciones establecidas en el manual interno de la empresa.	
			EFECTO	No cumplir con las funciones definidas para cada colaborador del departamento, crea confusión que podría llegar a evitar el cumplimiento de tareas y estarían realizando actividades que no ameriten.	
Evaluación de riesgos	7. Impacto de la materialización de los riesgos sobre los objetivos.	MR-1 MR-3	**CONDICIÓN**	En el departamento de finanzas y sistemas hay insuficiente seguimiento sobre el impacto que podría tener la materialización de los riesgos sobre los objetivos de la compañía.	Al jefe del departamento de finanzas y sistemas desarrollar un mapa de riesgos con escalas que identifiquen el impacto de los mismos, además, del seguimiento periódico por sus consecuencias.
			CRITERIO	Según la ISO 27001 un riesgo se puede determinar como cualquier evento que puede afectar los activos de información principalmente se relaciona con recursos humanos, eventos naturales o fallos técnicos. Las omisiones o descuido por parte del personal de la empresa, en definitiva, se busca elaborar una correcta gestión de riesgos.	
			CAUSA	El jefe del departamento asume que son riesgos controlables y que no tienen afectación a largo plazo.	
			EFECTO	Afectación directa a la compañía tanto económica, legal o retraso en sus actividades de materializarse la amenaza y dar paso al riesgo.	
	8. Procedimientos claves para la identificación de vulnerabilidades en los activos de información.	MR-2	**CONDICIÓN**	En el departamento de marketing tienen limitación en la definición de procedimientos claves para la identificación de vulnerabilidades en los activos de información	Al jefe de marketing supervisar el cumplimiento de quienes están a cargo de monitorear amenazas y vulnerabilidades en los activos de información.
			CRITERIO	Según la ISO 27001 un riesgo se puede determinar como cualquier evento que puede afectar los activos de información principalmente se relaciona con recursos humanos, eventos naturales o fallos técnico. Las omisiones o descuido por parte del personal de la empresa, en definitiva, se busca elaborar una correcta gestión de riesgos.	
			CAUSA	Falta de compromiso por parte del personal encargado para la creación de procesos claves en la identificación de vulnerabilidades	
			EFECTO	Materialización de amenazas que exploten las vulnerabilidades no controladas en los activos de información.	
Información y comunicación	9. Acciones de seguimiento para	MR-3	**CONDICIÓN**	En el departamento de finanzas no se realizan acciones de seguimiento que permitan validar el cumplimiento de los objetivos.	Al jefe de Sistemas diseñar indicadores internos que

	validar el cumplimiento de los objetivos		**CRITERIO**	Según las NCI apartado 410-13 Monitoreo y evaluación de procesos y servicios. La unidad de las TI expondrá a la alta dirección un informe de la supervisión del cumplimiento de los objetivos programados también se identificará e implantará acciones correctivas y mejoramiento en su desempeño.	permitan evaluar la eficiencia, el desempeño y la eficacia de las actividades y resultados sobre el cumplimiento de sus objetivos departamentales.
			CAUSA	No existen definidos indicadores en cuanto a la eficiencia y eficacia para el cumplimiento de los objetivos.	
			EFECTO	Deficiencia en las actividades para el cumplimiento de objetivos propuestos.	
Seguimiento y monitoreo	10. Procedimientos para la revisión de los procesos de control de las TIC	MR-3	**CONDICIÓN**	En el departamento de finanzas no se hace una revisión frecuente a los procesos de control de las TIC.	Al jefe de sistemas asignar a un responsable para gestionar los procesos y periodos de revisión de controles que están aplicando dentro del departamento de finanzas para un mejor y adecuado gobierno y gestión de las TIC.
			CRITERIO	Según las NCI apartado 410-04 Políticas y procedimientos la unidad de tecnología de la información establecerá los procedimientos que normen las actividades relacionadas con las TIC en la organización, los mismo que deberán ser actualizados de forma continua a ello se incorpora controles de aseguramiento y gestión de riesgos así miso directrices y patrones tecnológicos. En la ISO 27001 indica que es importante planificar, implementar y controlar los procesos de la organización además de hacer una valoración sobre los posibles riesgos en la seguridad de la información y el uso de los mismos.	
			CAUSA	Desconocimiento de los procesos para la revisión de los controles que están aplicando.	
			EFECTO	Impactos negativos sobre productividad, gobierno y gestión de las TIC.	

Elaborado por:	**LLSB**
Fecha:	1/7/2022
Revisado por:	**JEPP**
Fecha:	1/7/2022

3.3 Fase III

COMUNICACIÓN DE RESULTADOS

Para el desarrollo de esta fase se comunicó a los funcionarios de la compañía auditada los hallazgos encontrados expresados en los criterios, conclusiones y respectivas recomendaciones. Por tanto, se compone el informe presentado a continuación.

"BELÉN LAYEDRA" Auditor externo

INFORME GENERAL

AUDITORÍA DE SISTEMAS DE LA EMPRESA CORPORACIÓN IMPACTEX CIA. LTDA. POR EL PERÍODO COMPRENDIDO ENTRE EL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2021

SIGLAS Y/O ABREVIATURAS UTILIZADAS

Siglas y/o abreviaturas	Significado
SGSI	Sistema de Gestión de Seguridad de la Información
COSO	Committee of Sponsoring Organizations of the Tradeway Commission
SI	Sistemas de Información
TI	Tecnologías de Información
TIC	Tecnologías de la Información y la comunicación
ISO	Internacional Organization for Standardization
CGE	Contraloría General del Estado
NCI	Normas de Control Interno

ÍNDICE

CONTENIDO **PÁGINA**

Ambato, 31 de enero de 2022

Ing.

Betancourt Naranjo Kleber

Gerente general Corporación Impactex Cia. Ltda.

Presente. –

De mi consideración:

Hemos efectuado la evaluación de elementos importantes a través de la auditoría informática a la empresa Corporación Impactex Cia. Ltda., por el periodo comprendido entre el 1 de enero al 31 de diciembre de 2021.

El examen se efectuó de acuerdo con los, Estándares de normas ISO y marcos de referencia. Se ha considerado diversos factores informáticos que pueden estar influyendo en las operaciones de la empresa, así también que sus actividades se hayan ejecutado conforme a las disposiciones legales y reglamentarias vigentes, políticas y demás normas aplicables. El objetivo de la auditoría se enmarca en la verificación del cumplimiento de controles de las TIC, considerando como alcance la evaluación de áreas vulnerables, el nivel de confianza en cuanto al control interno informático, verificación de los activos de información, respuesta a riesgos relevantes, y herramientas de sistemas tanto física como lógica.

Debido a la naturaleza de la acción de control efectuada, los resultados se encuentran expresados en los criterios, conclusiones y recomendaciones que constan en el presente informe.

Atentamente,

Lcda. Layedra Lagua Soraya Belén

Auditor Senior "BELÉN LAYEDRA" Auditor externo
Ambato -Ecuador
REGISTRO 1643

RESULTADOS DEL EXAMEN

1. Políticas en el uso de equipos informáticos

Comentario

Hay escasa aplicación de políticas de restricción en el uso de equipos informáticos. Debido a que tienen equipos aislados y están a libre uso de los trabajadores de la compañía.

Conclusión

Según la norma ISO 27001 controles de la seguridad de los equipos informáticos. Los quipos necesitan atención particular y estar protegidos ante amenazas externas con el fin de evitar el acceso no autorizado o inapropiado, también de robos o pérdidas considerables. Con incumplimiento de esta norma la compañía tendría dificultad de identificar al usuario que le dio al uso al equipo informático en caso de pérdida o daño del mismo.

Recomendaciones

Dirigido al dpto. de sistemas

Mantener los soportes informáticos en un lugar cerrado al momento en que no sean utilizados, además aplicar un control de bloqueo de pantallas y designación de contraseñas para proteger los equipos que se encuentran sin vigilancia.

2. Aplicación de controles en la seguridad de información

Comentario

Se aplica controles medios en la seguridad de información reduciendo la prevención de riesgos. Debido a que no hay una cultura sobre la aplicación de controles eficientes y funcional, así como preventivos, correctivos o correctivos.

Conclusión

Según la norma ISO 27002 en todas las organizaciones se debe fijar una política sobre la seguridad de información, el mismo que contendrá la estructura, objetivos y la forma del control que tendría la información de la empresa. El desconocimiento de esta buena

práctica causa que la compañía no tenga la certeza de la efectividad del control ya que al aplicar un control medio no determina si la seguridad está bien o mal.

Recomendaciones

Dirigido al jefe de sistemas

Implementar una política sobre la seguridad de la información en la que se establezca los tipos de controles a aplicar tales como preventivos, detectivos y correctivos.

Ambiente de control

3. Evaluación periódica de los conocimientos de los miembros la compañía sobre el uso de las TIC.

Comentario

En el departamento de finanzas y marketing de la compañía tiene una débil evaluación periódica de los conocimientos de los miembros de la compañía sobre el uso de las TIC. Debido a la falta de un colaborador encargado de la revisión en cada departamento.

Conclusión

Según la norma ISO 9001: 2015 cláusula 7.1.6 no se consideró que el conocimiento organizacional es producto de la experiencia de cada individuo la misma que debe ser evaluada. De esta forma permitirá incorporar mejores conocimientos que serán aplicados en el desarrollo de procesos. Así mismo el mantenimiento, actualización y administración de la información es una vía que asegura la valides del conocimiento. Por tanto, la compañía tendría trabajadores con bajo rendimiento.

Recomendaciones

Dirigido al gerente de la compañía

Asignar personal para que se encargue de la evaluación periódica de los departamentos de marketing y financiero.

4. Inasistencia a las capacitaciones socializadas según el plan de capacitación

Comentario

En los departamentos de finanzas y marketing de la compañía no asisten las capacitaciones planificadas debido a que las capacitaciones son impartidas en horarios fuera de la jornada laboral.

Conclusión

Según las NCI apartado 410-15 Capacitación informática. Las capacitaciones serán impartidas tanto para el personal de TI así también para los usuarios por ello deberán contar con un plan de capacitación desarrollado con el apoyo del departamento del talento humano. Tiene el fin de satisfacer las necesidades de conocimientos específicos. Pasando por alto esta normativa el departamento de finanzas y marketing tendría una desventaja por sus trabajadores en actualización de temas en cuestión a nuevas tecnologías.

Recomendaciones

Dirigido al departamento de Talento Humano

Elaborar un cronograma de capacitación para cada departamento con horarios dentro de la jornada laboral.

4. Comunicación directa con los empleados sobre sus responsabilidades y lo que la dirección espera de ellos

Comentario

En el departamento de marketing hay escasa comunicación directa con los empleados sobre sus responsabilidades y lo que la dirección espera de ellos. Esto se debe a que se da una explicación general al momento de la contratación y no se realiza una retroalimentación sobre las responsabilidades que tiene cada empleado por parte del jefe del departamento.

Conclusión

Según la norma ISO 9001: 2015 especifica los aspectos de comunicación tanto internos como externos que determinará la eficiencia de la organización, además, que

se deben establecer canales de comunicación en el que se establezca el tiempo y el responsable de realizar la comunicación. Al desatender esta norma podría presentarse poca claridad en las actividades que deben realizar y por ende baja productividad para la compañía.

Recomendaciones

Dirigido al jefe de marketing

Especificar las responsabilidades de cada empleado y los objetivos a alcanzar al momento de incorporar a un empleado en su departamento.

5. Estructura, funciones y responsabilidades en el departamento.

Comentario

En el departamento de sistemas se modifican de forma constante su estructura, funciones y responsabilidades, esto se debe a que el departamento de sistemas no se está cumplimiento de las funciones establecidas en el manual interno de la empresa.

Conclusión

Según las NCI apartado 410-02. Segregación de funciones. Las funciones y responsabilidad deben ser definidos de forma clara y comunicados de manera formal que permitirá que los roles sean ejercidos con autoridad. Las responsabilidades pueden ser varias dentro de un mismo cargo. Las responsabilidades pueden ser varias dentro de un mismo cargo. Con el incumplimiento se esta norma la compañía no podrá cumplir con las funciones definidas para cada colaborador del departamento, crea confusión que podría llegar a evitar el cumplimiento de tareas y estarían realizando actividades que no ameriten.

Recomendaciones

Dirigido al jefe del departamento de sistemas

Supervisar que el personal a cargo realice las actividades según sus perfiles en cada una de sus tareas.

Evaluación de riesgos

6. Impacto de la materialización de los riesgos sobre los objetivos.

Comentario

En el departamento de finanzas y sistemas hay insuficiente seguimiento sobre el impacto que podría tener la materialización de los riesgos sobre los objetivos de la compañía. A causa de que el jefe del departamento asume que son riesgos controlables y que no tienen afectación a largo plazo.

Conclusión

Pasando por alto la norma ISO 27001 que establece que un riesgo se puede determinar como cualquier evento que puede afectar los activos de información principalmente se relaciona con recursos humanos, eventos naturales o fallos técnicos.

Las omisiones o descuido por parte del personal de la empresa, en definitiva, se busca elaborar una correcta gestión de riesgos. Esto puede llegar a afectar de forma directa a la compañía tanto económica, legal o retraso en sus actividades de materializarse la amenaza y dar paso al riesgo.

Recomendaciones

Dirigido al jefe del departamento de finanzas y sistemas

Desarrollar un mapa de riesgos con escalas que identifiquen el impacto de los mismos, además, del seguimiento periódico por sus consecuencias.

7. Procedimientos claves para la identificación de vulnerabilidades en los activos de información.

Comentario

En el departamento de marketing tienen limitación en la definición de procedimientos claves para la identificación de vulnerabilidades en los activos de información, consecuencia de la falta de compromiso por parte del personal encargado para la creación de procesos claves en la identificación de vulnerabilidades.

Conclusión

Según la ISO 27001 un riesgo se puede determinar como cualquier evento que puede afectar los activos de información principalmente se relaciona con recursos humanos,

eventos naturales o fallos técnico. Las omisiones o descuido por parte del personal de la empresa, en definitiva, se busca elaborar una correcta gestión de riesgos. Al no tomar en cuenta la norma citada anteriormente tendría un efecto en la materialización de amenazas que exploten las vulnerabilidades no controladas en los activos de información.

Recomendaciones

Dirigido al jefe de marketing

Supervisar el cumplimiento de quienes están a cargo de monitorear amenazas y vulnerabilidades en los activos de información.

Información y comunicación

8. Acciones de seguimiento para validar el cumplimiento de los objetivos

Comentario

En el departamento de finanzas no se realizan acciones de seguimiento que permitan validar el cumplimiento de los objetivos, debido a que no existen definidos indicadores en cuanto a la eficiencia y eficacia para el cumplimiento de los objetivos.

Conclusión

Según las NCI apartado 410-13 Monitoreo y evaluación de procesos y servicios. La unidad de las TI expondrá a la alta dirección un informe de la supervisión del cumplimiento de los objetivos programados también se identificará e implantará acciones correctivas y mejoramiento en su desempeño. Al no cumplirse con lo dispuesto en la NCI apartado 410-13 habría eficiencia en las actividades para el cumplimiento de objetivos propuestos.

Recomendaciones

Dirigido al jefe de Sistemas

Diseñar indicadores internos que permitan evaluar la eficiencia, el desempeño y la eficacia de las actividades y resultados sobre el cumplimiento de sus objetivos departamentales.

Seguimiento y monitoreo

9. Procedimientos para la revisión de los procesos de control de las TIC

Comentario

En el departamento de finanzas no se hace una revisión frecuente a los procesos de control de las TIC, debido al desconocimiento de los procesos para la revisión de los controles que están aplicando.

Conclusión

Según las NCI apartado 410-04 Políticas y procedimientos la unidad de tecnología de la información establecerá los procedimientos que normen las actividades relacionadas con las TIC en la organización, los mismo que deberán ser actualizados de forma continua a ello se incorpora controles de aseguramiento y gestión de riesgos así miso directrices y patrones tecnológicos. Así mismo en la ISO 27001 indica que es importante planificar, implementar y controlar los procesos de la organización además de hacer una valoración sobre los posibles riesgos en la seguridad de la información y el uso de los mismos. Al no aplicar la norma expuesta anteriormente el departamento tendría impactos negativos sobre productividad, gobierno y gestión de las TIC.

Recomendación

Dirigido al jefe de sistemas

Asignar a un responsable para gestionar los procesos y periodos de revisión de controles que están aplicando dentro del departamento de finanzas para un mejor y adecuado gobierno y gestión de las TIC.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

En la actualidad las compañías están expuestas a riesgos informáticos debido a la actualización tecnológica, protección de datos, ciberseguridad, fraudes, entre otros, por ello es importante la implementación de controles necesarios y adecuados para la protección en el uso de las Tecnologías de la Información y las comunicaciones, de modo que en el presente proyecto integrador se desarrolló la auditoria informática a la compañía Corporación Impactex Cia. Ltda. dando lugar a las conclusiones presentadas a continuación:

- Con la auditoría informática aplicada que la compañía conozca la situación actual sobre los recursos de las TIC, a través del análisis de hardware, software, red, personal, conocimientos y seguridad, además del cumplimento de normas y procedimientos. A través de los resultados se determina las mejoras e implementación de los cambios en el caso de ser necesarios.

- La compañía en la visita previa demostró tener principales falencias en el direccionamiento de las funciones y responsabilidades de la empresa, además de tener evaluaciones mínimas en sus controles, teniendo así una visión general sobre el estado de la empresa en lo referente a las TIC. Esto se logró gracias a la aplicación de herramientas y técnicas de auditoria que inicialmente se utilizó para el desarrollo de la fase de planificación, todo esto mediante la recopilación de información por medio las observación y entrevistas, siendo el punto de partida para realizar una evaluación adecuada y delimitar el proceso para realizar la fase de ejecución.

- En la fase de ejecución de la auditoria se detecta que la compañía presenta riesgos en cuanto a capacitaciones, comunicación directa con los directivos, determinación de funciones y en la identificación de vulnerabilidades todos estos moderados, que tienen la capacidad de ser mitigados. Además, la compañía no cuenta con un método de verificación del cumplimiento de controles lo que conlleva a que la compañía no cumpla con los objetivos propuestos. Los riesgos identificados se logran

por la aplicación del modelo COSO 2013 compuesto por 5 componentes basado en 17 principios básicos, gracias a este modelo se logra determinar el actuar correcto que debe tener la organización, orientada al logro de sus objetivos. Los controles internos establecidos determinan el compromiso de quienes conforman la empresa con sus valores éticos, estructura, responsabilidad, competencia y la identificación de posibles riesgos en sus activos y sistemas de información y en conjunto están encaminadas al desarrollo de sus actividades empresariales con la ayuda de herramientas tecnológicas.

- La comunicación de los resultados de auditoría se realiza a través de la redacción del informe detallando los hallazgos detectados en la fase de ejecución y recomendaciones sobre los mismos que a breves rasgos se pudo determinar que el mayor riesgo es en el factor humano particularmente en la definición de funciones. La comunicación oportuna permite que la compañía esté preparada ante riesgos que puedan afectar la integridad de las TIC.

4.2 Recomendaciones

A partir de la evaluación realizada a la compañía Corporación Impactex Cia. Ltda. a través de la aplicación de la auditoria informática se presenta las siguientes recomendaciones:

- En el estudio preliminar se detectó que la compañía no ha tenido ninguna auditoria informática en los años anteriores, por lo que se recomienda que se realice en un periodo anual con el fin de generar confianza a los usuarios en cuanto al cumplimiento de controles de las TIC.

- Con el fin de saber si los riesgos, amenazas y vulnerabilidades son manejables en cuanto a del cumplimiento de los controles de la TIC, se recomienda la aplicación de una matriz de seguimiento de controles de las TIC (anexo 4). De este modo se conocerá la eficiencia de los mismos.

- A partir de la ejecución de la auditoria se puede evidenciar que los principales riesgos de la compañía se presentan en el factor humano por ello se recomienda que la compañía debe realizar un control de los mismos en un periodo no mayor a 6 meses.

A partir del marco coso 2013 podrán establecer objetivos claros sobre el control interno de la compañía que estarán condicionados en 17 principios.

- Con la comunicación de resultados en el informe de auditoría se recomienda a la compañía realizar la fase de seguimiento, monitoreo y control de la implementación de las recomendaciones sugeridas en dicho informe (anexo 5).

REFERENCIAS BIBLIOGRÁFICAS

Abolacio Bosch, M. (2018). *Planificación de la auditoría. ADGD0108*. IC Editorial. https://elibro.net/es/ereader/uta/105602

Arcentales Fernández, D., & Caycedo Casas, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de Las Ciencias*, *3*(3 mon), 157–173. https://doi.org/10.23857/dom.cien.pocaip.2017.3.mono1.ago.157-173

Armas García, R. de. (2008). *Auditoría de gestión: conceptos y métodos*. Editorial Félix Varela. https://elibro.net/es/ereader/uta/71223

Bailon Lourido, W. A. (2019). Auditoria informática al control y mantenimiento de una infraestructura tecnológica. *Cienciamatria*, *5*(1), 73–87. https://doi.org/10.35381/cm.v5i1.248

Barberán Arboleda, R. P., & Díaz Díaz, F. J. (2019). La auditoría interna de sistemas en la gestión empresarial. *Cofin Habana*, *13*(2). https://doi.org/10.5281/zenodo.3471630

Bejarano, P. (n.d.). SAS - Statements on Auditing Standards o Las Declaraciones de Normas de Auditoría. *Apuntes de Auditoría y Finanzas*, 5. https://pedrobejarano.jimdofree.com/app/download/7303808662/Relación+Normas+SAS.pdf?t=1610674047&mobile=1

Bernal Torres, C. A. (2010). *Metodología de la investigación*. Pearson Educación. https://www.redalyc.org/pdf/5177/517751763017.pdf

Blanco Encinosa, L. J. (2008). *Auditoría y sistemas informáticos*. Editorial Félix Varela. https://elibro.net/es/ereader/uta/71229

Contraloría General del Estado. (2014). Normas De Control Interno De La Contraloria General Del Estado. *Registro Oficial*, *87*, 1–79. http://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cge_12_nor_con_int_400_cge.pdf

Couto Lorenzo, L. (2020). *Auditoría del sistema APPCC (2a. ed.)*. Ediciones Díaz de Santos. https://elibro.net/es/ereader/uta/129299

Davies, P. B. (2014). *Sistemas de Información* (Primera). Reverté. https://www.alphaeditorialcloud.com/library/publication/sistemas-de-

informacion-1597238824

Derrien, Y. (2009). *Técnicas de la auditoría informática*. marcombo boixareu editores. https://elibro.net/es/ereader/uta/45891

Espinoza Chuquimarca, M. O., Zurita Narváez, C. I., Andrade Ormaza, J. E., & Álvarez Erazo, J. C. (2020). El futuro de la auditoría y las innovaciones tecnológicas. *Ciencias Economicas Empresariales*, *6*, 316–339.

Faúndez Ugalde, A., Osman Hein, R., & Pino-Moya, M. (2018). La auditoría tributaria por sistemas electrónicos frente a los derechos de los contribuyentes. *Revista Chilena de Derecho y Tecnologia*, *7*(2), 113–135. https://doi.org/10.5354/0719-2584.2018.51099

I Aumatell, C. S. (2013). *Auditoría de la información identificar y explotar la información en las organizaciones* (Primera). Editorial UOC. https://elibro.net/es/ereader/uta/56771

Ignacio Tebar, B. J. (2016). *NIA 401 Auditoria en un Ambiente de Sistemas de Información por Computadora*. 2016. https://docplayer.es/22188026-Nia-401-auditoria-en-un-ambiente-de-sistemas-de-informacion-por-computadora.html

Instituto Mexicano de Contadores Públicos. (2020). *Guías de auditoría*. Instituto Mexicano de Contadores Públicos. https://elibro.net/es/ereader/uta/151224

ISO. (2013). ISO 27001:2013 Guía de implantación para la seguridad de la información. *Virtualex*, 30. https://app.virtualex.ec/app/visor.php?id=21459

ISO. (2015). Sistemas de gestión de la calidad - Requisitos. *Virtualex*, 30. https://app.virtualex.ec/app/visor.php?id=21111

Jimbo Santana, M. de J., Jimbo Santana, P. R., & Aguilar Viteri, E. A. (2017). Análisis de los Modelos de Capacidad para el proceso de gobierno de TI. *Revista Publicando*, *4*(10), 178–185.

Lapiedra Alcamí, R., Devece Carañana, C., & Guiral Herrando, J. (2016). *Introducción a la gestión de sistemas de información en la empresa*. D - Universitat Jaume I. Servei de Comunicació i Publicacions. https://elibro.net/es/ereader/uta/51689

Lezanski, P. D., Mattio, A. O., & Merino, S. B. (2016). *Sistemas de información*

contable II. Editorial Maipue. https://elibro.net/es/ereader/uta/77338

López Cruz, F. (2020). *Guía para elaborar el informe de auditoría independiente con base en Normas Internacionales de Auditoría*. Instituto Mexicano de Contadores Públicos. https://elibro.net/es/ereader/uta/174897

López Jara, A. A., Cañizares Roig, M., & Mayorga Díaz, M. P. (2018). La auditoría interna como herramienta de gestión para el control en los gobiernos autónomos descentralizados de la provincia de Morona Santiago. *Cuadernos de Contabilidad, 19*(47), 80–93. https://doi.org/10.11144/javeriana.cc19-47.aihg

Marco Galindo, M. J., Simó Marco, J. M., Blázquez Prieto, J., & Segret Sala, R. (2012). *Escaneando la informática*. Editorial UOC. https://elibro.net/es/ereader/uta/33518

Morles, V. (2001). Acerca de la ciencia y la tecnología: critica a los conceptos dominantes. *Acta Científica Venezolana*, 147–154.

Ocaña Fernández, Y., Valenzuela Fernández, A., Gálvez Suárez, E., Aguinaga Villegas, D., Nieto Gamboa, J., & López Echevarria, T. I. (2020). Gestión del conocimiento y tecnologías de la información y comunicación (TICs) en estudiantes de ingeniería mecánica. *Apuntes Universitarios, 10*(1), 77–88. https://doi.org/10.17162/revapuntes.v10i1.195

Pacheco Garisoain, M. L. (2016). *Tecnologías de la información y la comunicación*. Pearson Educación. https://elibro.net/es/ereader/uta/38062

Paredes Murcia, A., & León Cárdenas, M. J. (2021). La Auditoría fuente de información estratégica en la industria hotelera. *Turismo y Sociedad, 28*, 207–229. https://doi.org/10.18601/01207555.n28.10

Peña Vera, T. (2011). *Organización y representación del conocimiento: incidencias de las tecnología de la información y comunicación*. Alfagrama Ediciones. https://elibro.net/es/ereader/uta/188035

Piattini Velthuis, M., Del Pesos Navarro, E., & Del peso Ruiz, M. (2015). *Auditoría de tecnologías y sistemas de Información*. RA-MA. https://elibro.net/es/ereader/uta/106490

Rodríguez Labrada, Y. K., Cano Inclán, A., & Cuesta Rodríguez, F. (2019). Estado del arte de la Auditoría de Información. *E-Ciencias de La Información*, *9*(1649–

4142).

Sabillón, R., & Cano M., J. J. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. *RISTI - Revista Ibérica de Sistemas y Tecnologías de Información*, *32*, 33–48. https://doi.org/10.17013

Salas Nestares, C. De. (2007). *Guía para auditorías del sistema de gestión de prevención de riesgos laborables (Auditoría legal, OHSAS 18001 y criterios OIT)*. Ediciones Díaz de Santos. https://elibro.net/es/ereader/uta/53140

Sánchez Ch., W. (2021). *Teoría de la auditoría*. Grupo Editorial Nueva Legislación SAS. https://elibro.net/es/ereader/uta/188499

Santacruz Espinoza, J. J., Vega Abad, C. R., Pinos Castillo, L. F., & Cárdenas Villavicencio, O. E. (2017). Sistema cobit en los procesos de auditorías de los de sistemas informáticos. *Revista Ciencia e Investigación*, *2*(8), 65–68. https://doi.org/https://doi.org/10.26910/issn.2528-8083vol2iss8.2017pp65-68

Sevilla Tendero, J. (2015). *Auditoría de los sistemas integrados de gestión ISO 9001:2015, ISO 14001:2015, ISO 45001:2018*. FC Editorial. https://elibro.net/es/ereader/uta/130251

Tamayo Alzate, A. (1999). *¿Por que es imprescindible la auditoria de sistemas?* (pp. 71–75). McGraw Hill. https://repositorio.unal.edu.co/bitstream/handle/unal/60010/porqueesimprescindiblelaauditoria.pdf?sequence=1&isAllowed=y

Tamayo Alzate, A., & Duque M, N. D. (1999). *Planeación de la Auditoría de Sistemas* (pp. 42–47). McGraw Hill. https://repositorio.unal.edu.co/bitstream/handle/unal/60081/planeaciondelaauditoriadesistemas.pdf?sequence=1%0D%0A

Tejada, E. C. (2015). *Auditoría de seguridad informática (MF0487_3)*. IC Editorial. https://elibro.net/es/ereader/uta/44136

Universidad EAFIT Abierta al mundo. (2017). Normas ISO y su cobertura. *Revista Panorama Contable Contaduria Pública*, *1*, 1–10. http://www.eafit.edu.co/escuelas/administracion/publicaciones/panorama-contable/actualidad/Documents/Boletin-1-NORMAS-ISO-Y-SU-COBERTURA.pdf

Vasconcelos Santillán, J. (2016). *Tecnologías de la información* (Segunda). Grupo Editorial Patria. https://elibro.net/es/ereader/uta/40411

Vila Espeso, M. Á. (2007). *Auditorías internas de la calidad*. Ediciones Díaz de Santos. https://elibro.net/es/ereader/uta/52973

Yetano, A., & Castillejos, B. I. (2019). Auditorías de desempeño en América Latina. *Gestion y Política Píblica*, *28*(2), 407–440. https://doi.org/10.29265/gypp.v28i2.625

ANEXOS

Anexo 1. Archivo permanente

ARCHIVO PERMANENTE

INFORMACIÓN DE LA EMPRESA	
NOMBRE DE LA EMPRESA:	Corporación Impactex Cia. Ltda.
TIPO DE AUDITORÍA:	Auditoría Informática
PERÍODO AUDITADO:	Del 1 de enero al 31 de diciembre del 2021

ÍNDICE ARCHIVO PERMANENTE	AP
INFORMACIÓN GENERAL HISTÓRICO DE LA EMPRESA	APIG
Descripción de la empresa	APIG 1
Misión, Visión y Objetivos	APIG 2
Política de calidad	APIG 2
Reseña histórica	APIG 3
Organigrama de la empresa	APIG 4
Lista de funcionarios	APIG 5
INFORMACIÓN CONTABLE (SOFTWARE CONTABLE)	APIC
Descripción del software	APIC 1
Activos de Información	APIC 2
INFORMACIÓN SOBRE POLÍTICAS Y PROCEDIMIENTOS	APIP
Condiciones de venta	APIP 1
Marcas y logos	APIP 2

APIG 76

DESCRIPCIÓN DE LA EMPRESA

NOMBRE: CORPORACIÓN IMPACTEX CÍA. LTDA.

UBICACIÓN: Av. 22 de Enero y Circunvalación a 200 metros de la entrada a la parroquia Atahualpa junto al Complejo REVOLUTION - Ambato

Corporación Impactex es una empresa ecuatoriana, que se dedica a la fabricación de prendas de vestir de telas tejidas, de telas no tejidas, entre otras, para hombres, mujeres, niños y bebes. Además, a la venta al por mayor y menor de prendas de vestir, prendas de bioseguridad.

Su gerente y representante legal es el Ing. Klever Betancourt. Es una empresa establecida como una sociedad obligada a llevar contabilidad.

RAZÓN SOCIAL: CORPORACIÓN IMPACTEX CIA. LTDA.

APIG 2

MISIÓN

Somos una organización dedicada a la Innovación desarrollo y comercialización de marcas de moda con excelencia posicionándonos en los mercados nacionales y extranjeros para generar rentabilidad, sostenibilidad y crecimiento empresarial para nuestros clientes internos y externos.

VISIÓN

Ser un grupo empresarial líder en el mercado de moda con excelencia, responsabilidad social, empresarial y ambiental, internacionalizando nuestras marcas para crecer y consolidarnos, con nuestros consumidores neo tradicionales casuales.

OBJETIVO EMPRESARIAL

Generar recursos económicos por medio del desarrollo y la comercialización del portafolio de productos de Marcas, para satisfacer necesidades de vestimenta y estilo neo tradicional del mercado nacional e internacional.

POLÍTICA DE CALIDAD

Quienes integramos el GRUPO IMPACTEX estamos comprometidos a elaborar productos acordes a la moda innovando y diseñando prendas de calidad para cumplir las necesidades de nuestros clientes

APIG 3

RESEÑA HISTÓRICA

Impactex nace en la cuidad de Ambato en agosto del año 1999 su propietario el señor Milton Altamirano y su esposa Martha segura, inician sus actividades en el sector textil confeccionando y produciendo ropa interior masculina y camisetas unisex. En el transcurso de los primeros años fue ganando aceptación con sus clientes, generando el incremento de su producción, siendo el inicio para diversificar su línea de productos.

La visión y emprendimiento del señor Altamirano marca la pauta para que la ropa interior tenga una identidad propia, con calidad en las materias primas, diseños innovadores y a la moda que generen más consumidores, introduciéndose al mercado femenino y de niños.

Actualmente Impactex siendo fiel a su política de calidad, crea sus propias marcas legalmente patentadas, con el valor agregado de satisfacer las necesidades de sus clientes, tales como:

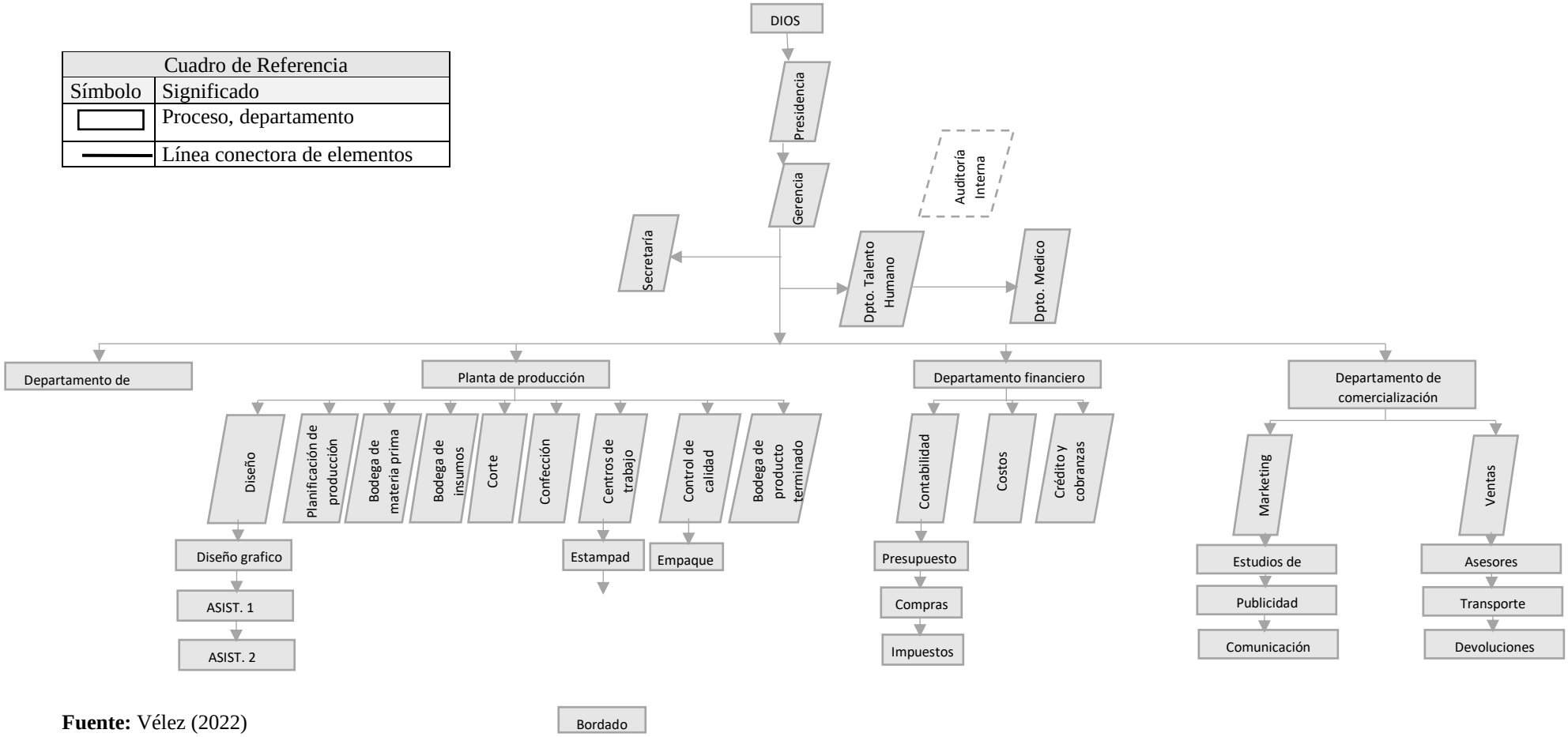
- Marca Mao
- Marca impacto
- Marca leidy Jasmín
- Marca mao junior e impactito
- Marca verito´s

ORGANIGRAMA ESTRUCTURAL DE LA EMPRESA

APIG 4

Figura 1. Estructura organizacional

Cuadro de Referencia	
Símbolo	Significado
▭	Proceso, departamento
───	Línea conectora de elementos



Fuente: Vélez (2022)

LISTA DE FUNCIONARIOS

APIG 5

1	Aguilar Aguilar Juan Carlos
2	Altamirano Segura Verónica Jazmina
3	Álvarez Herrera Kevin Ivan
4	Baño Luis Geovanny
5	Betancourt Naranjo Klever
6	Caisachana Serrano Alex Eduardo
7	Camacho Romero Patricio Rubén
8	Carvajal Cholo Silvia Mercedes
9	Casco Torres Jorge Luis
10	Chango Toapanta William Enrique
11	Chano Caiza Cesar David
12	Chano Caiza Cristian Xavier
13	Chato Conteron Lourdes Rocío
14	Chimborazo Tubon Narcisa Gabriela
15	Chugchilan Vega Margarita Mercedes
16	Chugchilan Vega Verónica Elizabeth
17	Chulco Yanchaliquin María Delia
18	Cisneros Caicedo Sofia Narcisa
19	Cunalata Paredes Cesar Iban
20	De la torre Llugcha Jonathan Wladimir
21	Espinoza Anchaluiza María Elvira
22	Estrella Mora Raúl Andrés
23	Freire Gavilánez Jenny Noemi
24	Gálvez Naranjo Doris Janeth
25	Gómez Guillin Wilmer Javier
26	Gómez Segura Álvaro Daniel
27	Guamán Miranda Betty Patricia
28	Guananga Chuqui Carmen Gabriela
29	Guananga López Valeria Carolina
30	Guangasi Tiban Viviana Elizabeth
31	Guillermo Correa Christian Mauricio
32	Hernández Jiménez Michael Mijaíl
33	Hurtado Suarez Alex Orlando
34	Hurtado Suarez Mario Cristóbal
35	Ichina Chimborazo Diego David
36	Ichina Chimborazo Édison Fabián
37	Intriago Mejía Ana Cristina
38	Iza Caguana Cristian José
39	Llundo Chochos Édison Ricardo
40	López Peña Édison Xavier
41	López Solís María Fernanda
42	Manobanda Jerez Maritza Fernanda
43	Martínez Villacis Andrea Cecibel
44	Mena Salazar Luis Javier
45	Mendoza Tipan Cesar Fabián
46	Miranda Villacis Kevin Andrés
47	Molina Naranjo Juan Fernando
48	Montoya Salcedo Cristina Alexandra
49	Moposita Quinga Cristina Aracelly
50	Nuela Moposita Jonathan Fernando
51	Olivarez Moya Sandra Narcisa
52	Oñate Galarza Jessica Tatiana
53	Orna Aguaiza Fredy Geovanny
54	Orna Ibarra Ivan Marcelo
55	Ortiz Quispe Rosa Abigail
56	Pilamunga Chimbolema Jessica Vanessa
57	Pilatasig Amancha Christian David
58	Pullupaxi Yansaguano Maribel Marlene
59	Punina Pomboza German Stalin
60	Punina Pomboza Ivonne victoria
61	Ramos Capuz Katherine Estefanía
62	Ronquillo Chango Mayra Beatriz
63	Ronquillo Cuspa Darío Javier
64	Ronquillo Paucar Fanny Margarita
65	Ronquillo Ruiz Édison Patricio
66	Ruiz Ronquillo Angelica Susana
67	Ruiz Ronquillo Oscar Edmundo
68	Sailema Lema Rosa Elena
69	Sánchez Moya Marlon Alexander
70	Sánchez Núñez Karen Anabell
71	Segura Correa Martha Bajira
72	Segura Correa Oscar Fernando
73	Segura Correa Rosario Enriqueta
74	Segura Manobanda Mayra Alejandra
75	Segura Vacacela Cristian David
76	Silva Aguacunchi Jessyca Abigail
77	Silva Mejía Michael Alejandro
78	Sisa Ramos Diego Xavier
79	Tobar Arcos Christian Eduardo
80	Tonato Delgado Silvana Esmeralda
81	Torres Morocho José Armando
82	Torres Tumailla Norma Faviola
83	Ushco Yanchapanta Franklin Rolando
84	Vargas Ramos Juan Andrés
85	Vargas Torres José Luis
86	Vásquez Minda Vanessa Michelle
87	Villamarin Toapanta Elvia Noemi

DESCRIPCIÓN DEL SISTEMA CONTABLE
UTILIZADO EN CORPORACIÓN IMPACTEX CIA. LTDA.

APIC 1

CORPORACIÓN IMPACTEX CÍA. LTDA. cuenta con un sistema contable JIREH - WINDOWS SERVER 2019 que está integrado con otros sistemas informáticos de la compañía su función principal es la gestión contable y financiera con un tipo de arquitectura en capas. El sistema operativo del servidor es Windows Server 2008 y para el cliente Windows 7, además, su almacenamiento tiene un servidor propio. Este sistema emite reportes en hojas de cálculo , tiene respaldos que se conserva anualmente , también dispone de facturación electrónica.

MÓDULOS

Nombre del módulo	Principal funcionalidad
INVENTARIOS	Gestiona la información de cada una de las bodegas y sus transacciones
FACTURACIÓN	Módulo para toma de pedidos y facturación de producto terminado
CUENTAS POR COBRAR	gestiona la cartera, pagos y estado de cuenta de clientes
CUENTAS POR PAGAR	Gestiona facturas de compra, cartera, pagos y estado de cuenta de proveedores
TESORERÍA	Gestiona información de cobros y pagos
CONTABILIDAD	Gestiona la información contable de todos los módulos
GESTIÓN HUMANA	Gestiona la información del personal, incluido roles de pago

CORPORACIÓN IMPACTEX CÍA. LTDA. cuenta con un segundo sistema contable para el departamento de producción INCORP que está integrado con otros sistemas informáticos de la compañía su función principal es la gestión contable y financiera con un tipo de arquitectura en capas. El sistema operativo del servidor es Windows Server 2019 y para el cliente Windows 7,10,11 además, su almacenamiento tiene un servidor propio y nube privada. Este sistema emite reportes en hojas de cálculo y pdf, tiene respaldos que se conserva anualmente.

MÓDULOS

Nombre del módulo	Principal funcionalidad
DISEÑO MODAS	Gestiona la información de cada una de las bodegas y sus transacciones
FORMULACIONES	Módulo para toma de pedidos y facturación de producto terminado
BODEGAS	Gestiona la cartera, pagos y estado de cuenta de clientes
CORTE Y MAQUILAS	Gestiona facturas de compra, cartera, pagos y estado de cuenta de proveedores
PRODUCCIÓN	Gestiona información de cobros y pagos
MANO DE OBRA	Gestiona la información contable de todos los módulos
CONTROL DE CALIDAD	Gestiona la información del personal, incluido roles de pago

LISTADO DE ACTIVOS DE INFORMACIÓN

APIC 2

A continuación, se presenta un detalle de los equipos con que cuenta la empresa:

Activo de Información	**Departamento**
5 computadoras de escritorio y 2 impresoras Epson y Ricoh	Administración
1 computador portátil y 1 impresora Epson	Bodega
2 computadoras de escritorio	Bodega e insumos
1 computador de escritorio	Calidad
1 computador de escritorio	Call center
1 computador de escritorio	Contabilidad
2 computadoras de escritorio, 1 computador portátil y 1 impresora Epson	Corte
5 computadoras de escritorio y 1 impresora Epson	Diseño
3 computadoras de escritorio y 3 impresoras Epson	Facturación
1 computador de escritorio	Guardianía
1 computador de escritorio, 1 computador portátil y 1 impresora Epson	Insumo
3 computadoras de escritorio, 1 computador portátil y 2 impresoras Xerox y Epson	Marketing
1 computador de escritorio	Planta de producción
2 computadoras de escritorio y 2 impresoras Epson y Zebra	Showroom
1 computador de escritorio y 1 impresora Epson	Talento humano
Windows 10	Administración, Bodega, Bodega e insumos, Calidad, Call center, Contabilidad, Corte. Diseño, Facturación, Guardianía, Insumo, Marketing, Planta de producción, Showroom y Talento humano.
Sistema contable financiero JIREH - WINDOWS SERVER 2019	Contabilidad – facturación
Sistema contable de producción INCORP	Producción
Microsoft Office	
Páginas electrónicas de venta	
Correos electrónicos	
Redes Sociales	
Lector de barra	
Parlante amplificador	
Discos externos de almacenamiento	
Proyector	
Cajón para dinero	
11 Teléfonos convencionales	
Router	
Antena wifi	
Cámaras de seguridad	
Software	
Generador de luz	
Antivirus	
Factor humano (directivos, jefes departamentales, asesores, operarios)	

APIP 1

OBJETIVO COMERCIAL

Comercializar prendas de ropa interior acordes a la moda, marcando la diferencia del buen vestir interior en el mercado nacional.

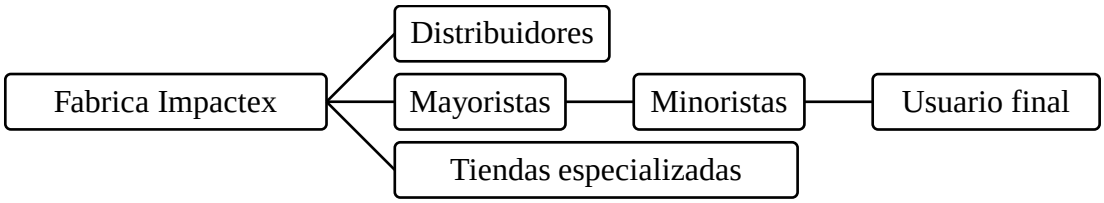
DESCRIPCIÓN DEL CLIENTE

Consumidor de prendas de edad comprendida de 15 a 38 años de educación media y superior, con gusto de moda e innovadores, que viven en zonas urbanas y rurales, con ingresos de economía media

CANAL DE COMERCIALIZACIÓN

Impactex tiene definido su canal de comercialización siguiendo el siguiente esquema

Figura 1. Esquema de comercialización



Fuente: Vélez (2022)

MARCAS Y PRODUCTOS

APIP 2

A continuación, se detalla las marcas de mayor éxito de la empresa:

Logos	Descripción
	Marca Mao.- ropa interior para hombres de algodón con sus líneas bóxer, calzoncillos, camisetas, dividís marca que actualmente lidera el mercado nacional y con miras de exportación a países como Perú y Colombia.
	Marca impacto: para el segmento masculino en poli algodón de precios medios económicos en líneas como bóxer calzoncillo tanga y dividí.
	Marca leidy Jasmín: ropa interior para mujeres con estilos acordes a la moda prendas confortables con gran dedicación y calidad.
	Marca mao junior e impactito : para el segmento infantil de niños con coloridos diseños y atractivos modelos que son cada vez más aceptados para la sociedad.
	Marca verito´s: Ropa interior para niñas con toques de delicadeza y variedad de diseños que cuidan la ternura de la infancia.
	IMPACTEX: Logo principal de la compañía.

Elaborado por: Layedra (2022)

Anexo 2. Guía de entrevista

Interrogante	Respuesta	
1. ¿La empresa ha tenido una auditoría informática en los años anteriores?	☐ SI	☑ NO
2. ¿La empresa cuenta con un inventario de todos los equipos informáticos que posee?	☑ SI	☐ NO
3. ¿El departamento de sistemas cuenta con un administrador de red informático?	☑ SI	☐ NO
4. ¿Utilizan dispositivos especializados para las conexiones del exterior?	☑ SI	☐ NO
5. ¿Se realiza mantenimiento a los activos de información?	☑ SI	☐ NO
6. ¿Se analizan aplicaciones instaladas?	☑ SI	☐ NO
En caso de responder Si, contestar la siguiente pregunta		
7. ¿Con que frecuencia se realiza el análisis?	☐ Diariamente ☐ Una vez a la semana ☑ Cada 15 días ☐ Una vez al año	
8. ¿Se evalúan técnicas y comportamiento del sistema?	☑ SI	☐ NO
9. ¿Se realiza planificación en los procedimientos de utilización de las TIC?	☑ SI	☐ NO
10. ¿Están definidas las funciones de todos los trabajadores del departamento de Sistemas?	☐ SI	☑ NO
11. ¿Tienen respaldo de la información?	☑ SI	☐ NO
En caso de responder Si, contestar la siguiente pregunta		
12. ¿Qué tipos de respaldo utiliza?	☑ Copia de seguridad completa ☐ Copia de seguridad incremental ☐ Copia de seguridad diferencial	
13. ¿Existe controles en los procedimientos informáticos?	☑ SI	☐ NO
14. ¿Realizan reuniones para dar seguimientos a los procedimientos?	☑ SI	☐ NO
En caso de responder Si, contestar la siguiente pregunta		
15. ¿Con que frecuencia se realiza las reuniones?	☑ Un vez a la semana ☐ Cada 15 días ☐ Una vez al mes ☐ Una vez al año ☐ Otros	
16. ¿Se realizan cambios en los procedimientos?	☑ SI	☐ NO
17. ¿Los cambios son debidamente autorizados?	☑ SI	☐ NO
18. ¿Realizan mantenimiento en los programas utilizados por la empresa?	☐ SI	☑ NO
En caso de responder Si, contestar la siguiente pregunta		
19. ¿Qué tipo de mantenimiento utilizan?	☐ Preventivo ☐ Correctivo ☑ Medio	
20. ¿En la gestión de la información están normados bajo la ISO/IEC 27001?	☐ SI	☑ NO
21. ¿Los controles son establecidos con apoyo de la ISO 27002?	☐ SI	☑ NO
22. ¿Cuenta con claves de seguridad?	☑ SI	☐ NO
23. ¿Hay restricciones sobre el uso de equipos informáticos que tiene la empresa?	☐ SI	☑ NO
24. ¿Se evalúa la efectividad de los controles? Sustente su respuesta.	☐ SI	☑ NO
Porque:	Algunos procesos manejan autorización y autenticación, pero en su mayoría el control es nulo.	
25. ¿Se comprueba si las acciones son efectivas, sin involucrar la operatividad?	☐ SI	☑ NO
26. ¿Se comprueba la seguridad, integridad y autenticidad de datos?	☐ SI	☑ NO
27. ¿Tienen un método de medir la operatividad de los dispositivos?	☐ SI	☑ NO
28. ¿Se evalúa el conocimiento de los trabajadores?	☑ SI	☐ NO
29. ¿Se revisa la metodología que se utiliza para el desarrollo de los diferentes proyectos?	☑ SI	☐ NO
30. ¿Se revisa los procesos de la seguridad informática físicos y lógicos?	☑ SI	☐ NO

31. ¿Implementan nuevos sistemas de información?	☑ SI	☐ NO
32. ¿Se socializa a los demás departamentos los procedimientos?	☑ SI	☐ NO
33. ¿Los directivos actúan bajo el principio de prevención de riesgos?	☑ SI	☐ NO
34. ¿Se siente incentivado para la realización de sus actividades?	☐ SI	☑ NO
35. ¿Recibe bonificaciones por buen desempeño?	☐ SI	☑ NO
36. ¿Los procedimientos están encaminados al cumplimiento de leyes, normas y reglamentos frente a las autoridades competentes?	☑ SI	☐ NO
37. Tiene recomendaciones para mejorar la gestión de las tecnologías de la información	✓ Contratar personal dedicado ✓ Capacitar a los usuarios en la resolución de pequeños conflictos informáticos ✓ Tener una cultura de sostenibilidad informática	
38. ¿Según su criterio cual es el área que presenta mayor riesgo dentro del departamento de sistemas?	El área de desarrollo al no tener claro las actividades del área, y deslindar ciertas actividades importantes, por problemas pequeños que a la suma consumen el día a día.	
39. Nombre del encuestado: Josué Vélez		
40. Cargo: Asistente de sistemas		

Anexo 3. Cuestionario marco COSO 2013

CUESTIONARIO DE CONTROL INTERNO
Departamento de Finanzas

COMPONENTE	PRINCIPIOS	No.	DESCRIPCIÓN	RESPUESTAS					COMENTARIOS
				SI	NO	N/A	PT	CT	
AMBIENTE DE CONTROL	Principio 1. Demuestra compromiso con la integridad y los valores éticos	1	¿ El comportamiento y las decisiones de la Gerencia y los niveles de supervisión reflejan su compromiso con el cumplimiento de la ética y los valores?	x			1	1	
		2	¿La asignación de responsabilidad y el establecimiento de políticas, son la base para el seguimiento de las actividades en el uso de las tecnologías?	x			1	1	
		3	¿La compañía cuenta con políticas que incluyan los controles de TI?	x			1	1	
		4	¿Se informa sobre las acciones disciplinarias en el caso de incumplimiento de las normas de comportamiento?	x			1	1	
	Principio 2. Ejerce Responsabilidad de Supervisión	5	¿Se evalúan periódicamente los conocimientos de los miembros la compañía sobre el uso de las TIC?		x		1	0	
		6	¿Los miembros de la compañía son independientes a la administración y por tanto sus decisiones son libres y objetivas?	x			1	1	
	Principio 3. La Gerencia Establece estructura, autoridad, y responsabilidad	7	¿La estructura organizativa y funcional permite el cumplimiento de sus objetivos?	x			1	1	
		8	¿La compañía cuenta con especialistas con conocimientos sobre las TI sea internos o externos?	x			1	1	
		9	¿En el desarrollo de estrategias del departamento consideran la inversión y uso de las TI?			x	0	0	
		10	¿Se modifica de forma constante la estructura, funciones y responsabilidades en la compañía?		x		1	0	
	Principio 4. La organización demuestra compromiso por reclutar y mantener	11	¿ La empresa tiene un proceso definido para el reclutamiento de nuevos empleados, según los requerimientos departamentales?	x			1	1	
		12	¿La empresa mantiene comunicación directa con los empleados enfatizando sus responsabilidades y lo que la dirección espera de ellos?	x			1	1	

	colaboradores competentes.	13	¿Se formula un plan de capacitación para el personal de la compañía?			x	0	0	
		14	¿Se socializa el plan de capacitación al personal de la compañía?		x		1	0	
	Principio 5. Hace cumplir con la responsabilidad	15	¿Se realiza un reconocimiento a los colaboradores que se destaquen en el cumplimiento de las normas éticas, así como en el desempeño esperado?		x		1	0	
		16	¿Los empleados son conscientes del compromiso laboral con la empresa considerando que de existir un comportamiento no aceptable o incumplimiento a las normas internas son motivo de sanciones?	x			1	1	
			TOTAL				**14**	**10**	
EVALUACIÓN DE RIESGOS	**Principio 6. La organización define objetivos claros y relevantes, que permiten la identificación y evaluación de riesgos asociados.**	1	¿ Los objetivos establecidos están alineados con la estrategia de la compañía y con las normas internas y externas que la regulan?	x			1	1	
		2	¿Se ha definido procedimientos claves para la identificación de vulnerabilidades en sus activos de información?	x			1	1	
	Principio 7. Se identifican y analizan los riesgos para el logro de los objetivos.	3	¿Los directivos de la compañía identifican los riesgos que pueden afectar el logro de los objetivos institucionales, en base a los factores internos o externos?	x			1	1	
		4	¿Se conocen los controles que la compañía aplica relacionados con los riesgos identificados?	x			1	1	
		5	¿La compañía cuenta con un sistema de seguridad y vigilancia para la prevención de amenazas que puedan atentar a la integridad de su personal?	x			1	1	
	Principio 8. Se evalúa el riesgo de Fraude	6	¿Tienen mecanismos adecuados para identificar riesgos internos?	x			1	1	
		7	¿Se consideran diferentes riesgos de fraude, tal como la corrupción y la pérdida de activos de información, en el análisis de riesgos de la compañía?	x			1	1	
		8	¿Se evalúa los riesgos por ataques cibernéticos?			x	0	0	
		9	¿El departamento ha sufrido fraude o robo de información por parte de un colaborador interno?		x		1	0	

	Principio 9. Se identifican y analizan cambios importantes que puedan impactar el Sistema de Control Interno	10	¿Se realiza un seguimiento del impacto que podrían tener la materialización de los riesgos sobre los objetivos del departamento?		x		1	0	
		11	¿Se consideran criterios importantes de evaluación a recursos humanos, presupuesto, sistemas de información diseño de procesos, claves de seguridad, respaldos, mantenimiento y la seguridad, integridad y autenticidad de datos?	x			1	1	
		12	¿La empresa realiza comprobación periódica de la seguridad, integridad y autenticidad de datos?	x			1	1	
			TOTAL				**11**	**9**	
ACTIVIDADES DE CONTROL	**Principio 10. Seleccionar y Desarrollar Actividades de Control**	1	¿Las actividades de control aplicados en la empresa son tanto preventivos como correctivas?	x			1	1	
		2	¿Tienen manuales, instructivos o normas de forma escrita que regulen el desarrollo de las diferentes actividades de trabajo con el uso de las TIC?	x			1	1	
		3	¿La compañía tiene instaladas cámaras de seguridad como procedimiento de control preventivo ante cualquier anomalía en sus instalaciones?	x			1	1	
	Principio 11. La organización selecciona y desarrolla controles generales sobre tecnología	4	¿Se han implementado controles orientados sobre el desarrollo, compra y mantenimiento de programas e infraestructura de TI?	x			1	1	
		5	¿Se asegura lógica y físicamente los equipos e infraestructura de TI?	x			1	1	
		6	¿ Se utilizan mecanismos de control para el acceso y autenticación de usuarios no autorizados?	x			1	1	
		7	¿Se ha implementado un software antivirus?	x			1	1	
		8	¿Se realiza mantenimiento periódico al software antivirus?	x			1	1	
		9	¿Se define perfiles y permisos de usuario en cada una de las herramientas de apoyo tecnológico de acuerdo con el rol desempeñado?	x			1	1	
		10	¿Se han implementado controles orientados a la adquisición y mantenimiento de los activos de información?	x			1	1	
	Principio 12. Implementación de las actividades de control,	11	¿Los responsables de cada departamento diseñan controles relacionados con planes y programas de la actividad que desarrolla?	x			1	1	

	por medio de políticas y procedimientos.	12	¿Se ha dado seguimiento a la rotación de tareas, de manera que tenga independencia, separación de funciones incompatibles?			x	0	0	
			TOTAL				**11**	**11**	
INFORMACIÓN Y COMUNICACIÓN	**Principio 13. Generar y utilizar información relevante y de calidad.**	1	¿Se identifica y presenta con seguridad la información, generada dentro de la compañía, esencial para el logro de los objetivos de la compañía?	x			1	1	
		2	¿La calidad y oportunidad de la información permite la toma de decisiones adecuada, tanto hacia la máxima autoridad como a los jefes de los departamentos?	x			1	1	
		3	¿Existe la suficiente comunicación que facilite al personal de la compañía a cumplir sus funciones?	x			1	1	
	Principio 14. Información Interna	4	¿En el departamento se ha definido los métodos de comunicación que son válidos en cada uno de los procesos, tales como correos electrónicos, memorandos internos, comités, intranet y mensajes de texto, entre otros?	x			1	1	
		5	¿La información se facilita con el detalle adecuado para los distintos niveles de gestión?	x			1	1	
		6	¿Tienen un protocolo para la comunicación de información a los niveles superiores de la compañía?	x			1	1	
		7	¿Se realizan acciones de seguimiento, que permitan validar el cumplimiento de los objetivos de la organización?		x		1	0	
	Principio 15. Comunicación Externa o a terceros	8	¿Se han definido los responsables de la recepción de información de los entes externos, reduciendo la posibilidad de no atender un requerimiento por falta de gestión o conocimiento al interior de la organización?	x			1	1	
			TOTAL				**8**	**7**	
SEGUIMIENTO Y MONITOREO	**Principio 16. Evaluaciones Continuas o Independientes**	1	¿Se realizan evaluaciones de seguimiento continuo sobre las actividades, que cada una de las unidades realiza, y que permitan aplicar medidas oportunas?	x			1	1	
		2	¿Existen procedimientos para que la dirección revise los procesos de control de las TIC, para asegurarse de su cumplimiento del modo esperado?		x		1	0	
	Principio 17. Evaluación y comunicación de las	3	¿Los resultados de las evaluaciones realizadas, bien sea independientes o continuas son revisadas por los directivos o la Gerencia?	x			1	1	

	deficiencias encontradas.	4	¿La empresa realiza un seguimiento frecuente a las deficiencias encontradas en procesos internos que afecten al desarrollo normal de sus actividades?	x			1	1	
		5	¿Se aplica procedimientos para la mejora continua de las actividades internas?	x			1	1	
			TOTAL				**5**	**4**	

TOTAL GENERAL		**49**	**41**

CUESTIONARIO DE CONTROL INTERNO

Departamento de Marketing

COMPONENTE	**PRINCIPIOS**	**No.**	**DESCRIPCIÓN**	**RESPUESTAS**					**COMENTARIOS**
				SI	**NO**	**N/A**	**PT**	**CT**	
AMBIENTE DE CONTROL	**Principio 1. Demuestra compromiso con la integridad y los valores éticos**	1	¿ El comportamiento y las decisiones de la Gerencia y los niveles de supervisión reflejan su compromiso con el cumplimiento de la ética y los valores?	x			1	1	
		2	¿La asignación de responsabilidad y el establecimiento de políticas, son la base para el seguimiento de las actividades en el uso de las tecnologías?	x			1	1	
		3	¿La compañía cuenta con políticas que incluyan los controles de TI?	x			1	1	
		4	¿Se informa sobre las acciones disciplinarias en el caso de incumplimiento de las normas de comportamiento?	x			1	1	
	Principio 2. Ejerce Responsabilidad de Supervisión	5	¿Se evalúan periódicamente los conocimientos de los miembros la compañía sobre el uso de las TIC?		x		1	0	
		6	¿Los miembros de la compañía son independientes a la administración y por tanto sus decisiones son libres y objetivas?	x			1	1	
	Principio 3. La Gerencia Establece estructura,	7	¿La estructura organizativa y funcional permite el cumplimiento de sus objetivos?	x			1	1	
		8	¿La compañía cuenta con especialistas con conocimientos sobre las TI sea internos o externos?	x			1	1	

	autoridad, y responsabilidad	9	¿En el desarrollo de estrategias del departamento consideran la inversión y uso de las TI?	x			1	1	
		10	¿Se modifica de forma constante la estructura, funciones y responsabilidades en la compañía?		x		1	0	
	Principio 4. La organización demuestra compromiso por reclutar y mantener colaboradores competentes.	11	¿ La empresa tiene un proceso definido para el reclutamiento de nuevos empleados, según los requerimientos departamentales?	x			1	1	
		12	¿La empresa mantiene comunicación directa con los empleados enfatizando sus responsabilidades y lo que la dirección espera de ellos?		x		1	0	
		13	¿Se formula un plan de capacitación para el personal de la compañía?			x	1	1	
		14	¿Se socializa el plan de capacitación al personal de la compañía?		x		1	0	
	Principio 5. Hace cumplir con la responsabilidad	15	¿Se realiza un reconocimiento a los colaboradores que se destaquen en el cumplimiento de las normas éticas, así como en el desempeño esperado?		x		1	0	
		16	¿Los empleados son conscientes del compromiso laboral con la empresa considerando que de existir un comportamiento no aceptable o incumplimiento a las normas internas son motivo de sanciones?	x			1	1	
			TOTAL				**16**	**11**	
EVALUACIÓN DE RIESGOS	**Principio 6. La organización define objetivos claros y relevantes, que permiten la identificación y evaluación de riesgos asociados.**	1	¿ Los objetivos establecidos están alineados con la estrategia de la compañía y con las normas internas y externas que la regulan?	x			1	1	
		2	¿Se ha definido procedimientos claves para la identificación de vulnerabilidades en sus activos de información?		x		1	0	
	Principio 7. Se identifican y analizan los riesgos para el logro de los objetivos.	3	¿Los directivos de la compañía identifican los riesgos que pueden afectar el logro de los objetivos institucionales, en base a los factores internos o externos?	x			1	1	
		4	¿Se conocen los controles que la compañía aplica relacionados con los riesgos identificados?	x			1	1	
		5	¿La compañía cuenta con un sistema de seguridad y vigilancia para la prevención de amenazas que puedan atentar a la integridad de su personal?	x			1	1	

	Principio 8. Se evalúa el riesgo de Fraude	6	¿Tienen mecanismos adecuados para identificar riesgos internos?			x	0	0	
		7	¿Se consideran diferentes riesgos de fraude, tal como la corrupción y la pérdida de activos de información, en el análisis de riesgos de la compañía?	x			1	1	
		8	¿Se evalúa los riesgos por ataques cibernéticos?	x			1	1	
		9	¿El departamento ha sufrido fraude o robo de información por parte de un colaborador interno?			x	0	0	
	Principio 9. Se identifican y analizan cambios importantes que puedan impactar el Sistema de Control Interno	10	¿Se realiza un seguimiento del impacto que podrían tener la materialización de los riesgos sobre los objetivos del departamento?	x			1	1	
		11	¿Se consideran criterios importantes de evaluación a recursos humanos, presupuesto, sistemas de información diseño de procesos, claves de seguridad, respaldos, mantenimiento y la seguridad, integridad y autenticidad de datos?	x			1	1	
		12	¿La empresa realiza comprobación periódica de la seguridad, integridad y autenticidad de datos?	x			1	1	
			TOTAL				**10**	**9**	
ACTIVIDADES DE CONTROL	**Principio 10. Seleccionar y Desarrollar Actividades de Control**	1	¿Las actividades de control aplicados en la empresa son tanto preventivos como correctivas?	x			1	1	
		2	¿Tienen manuales, instructivos o normas de forma escrita que regulen el desarrollo de las diferentes actividades de trabajo con el uso de las TIC?	x			1	1	
		3	¿La compañía tiene instaladas cámaras de seguridad como procedimiento de control preventivo ante cualquier anomalía en sus instalaciones?	x			1	1	
	Principio 11. La organización selecciona y desarrolla controles generales sobre tecnología	4	¿Se han implementado controles orientados sobre el desarrollo, compra y mantenimiento de programas e infraestructura de TI?	x			1	1	
		5	¿Se asegura lógica y físicamente los equipos e infraestructura de TI?	x			1	1	
		6	¿ Se utilizan mecanismos de control para el acceso y autenticación de usuarios no autorizados?	x			1	1	
		7	¿Se ha implementado un software antivirus?	x			1	1	
		8	¿Se realiza mantenimiento periódico al software antivirus?	x			1	1	

		9	¿Se define perfiles y permisos de usuario en cada una de las herramientas de apoyo tecnológico de acuerdo con el rol desempeñado?	x			1	1	
		10	¿Se han implementado controles orientados a la adquisición y mantenimiento de los activos de información?	x			1	1	
	Principio 12. Implementación de las actividades de control, por medio de políticas y procedimientos.	11	¿Los responsables de cada departamento diseñan controles relacionados con planes y programas de la actividad que desarrolla?	x			1	1	
		12	¿Se ha dado seguimiento a la rotación de tareas, de manera que tenga independencia, separación de funciones incompatibles?	x			1	1	
			TOTAL				**12**	**12**	
INFORMACIÓN Y COMUNICACIÓN	**Principio 13. Generar y utilizar información relevante y de calidad.**	1	¿Se identifica y presenta con seguridad la información, generada dentro de la compañía, esencial para el logro de los objetivos de la compañía?	x			1	1	
		2	¿La calidad y oportunidad de la información permite la toma de decisiones adecuada, tanto hacia la máxima autoridad como a los jefes de los departamentos?	x			1	1	
		3	¿Existe la suficiente comunicación que facilite al personal de la compañía a cumplir sus funciones?	x			1	1	
	Principio 14. Información Interna	4	¿En el departamento se ha definido los métodos de comunicación que son válidos en cada uno de los procesos, tales como correos electrónicos, memorandos internos, comités, intranet y mensajes de texto, entre otros?	x			1	1	
		5	¿La información se facilita con el detalle adecuado para los distintos niveles de gestión?	x			1	1	
		6	¿Tienen un protocolo para la comunicación de información a los niveles superiores de la compañía?	x			1	1	
		7	¿Se realizan acciones de seguimiento, que permitan validar el cumplimiento de los objetivos de la organización?	x			1	1	
	Principio 15. Comunicación Externa o a terceros	8	¿Se han definido los responsables de la recepción de información de los entes externos, reduciendo la posibilidad de no atender un requerimiento por falta de gestión o conocimiento al interior de la organización?	x			1	1	
			TOTAL				**8**	**8**	

SEGUIMIENTO Y MONITOREO	**Principio 16. Evaluaciones Continuas o Independientes**	1	¿Se realizan evaluaciones de seguimiento continuo sobre las actividades, que cada una de las unidades realiza, y que permitan aplicar medidas oportunas?	x			1	1	
		2	¿Existen procedimientos para que la dirección revise los procesos de control de las TIC, para asegurarse de su cumplimiento del modo esperado?	x			1	1	
	Principio 17. Evaluación y comunicación de las deficiencias encontradas.	3	¿Los resultados de las evaluaciones realizadas, bien sea independientes o continuas son revisadas por los directivos o la Gerencia?	x			1	1	
		4	¿La empresa realiza un seguimiento frecuente a las deficiencias encontradas en procesos internos que afecten al desarrollo normal de sus actividades?	x			1	1	
		5	¿Se aplica procedimientos para la mejora continua de las actividades internas?	x			1	1	
			TOTAL				**5**	**5**	

TOTAL GENERAL	**51**	**45**

CUESTIONARIO DE CONTROL INTERNO
DEPARTAMENTO DE SISTEMAS

COMPONENTE	PRINCIPIOS	No.	DESCRIPCIÓN	RESPUESTAS					COMENTARIOS
				SI	NO	N/A	PT	CT	
AMBIENTE DE CONTROL	**Principio 1. Demuestra compromiso con la integridad y los valores éticos**	1	¿ El comportamiento y las decisiones de la Gerencia y los niveles de supervisión reflejan su compromiso con el cumplimiento de la ética y los valores?	x			1	1	
		2	¿La asignación de responsabilidad y el establecimiento de políticas, son la base para el seguimiento de las actividades en el uso de las tecnologías?	x			1	1	
		3	¿La compañía cuenta con políticas que incluyan los controles de TI?	x			1	1	
		4	¿Se informa sobre las acciones disciplinarias en el caso de incumplimiento de las normas de comportamiento?	x			1	1	

	Principio 2. Ejerce Responsabilidad de Supervisión	5	¿Se evalúan periódicamente los conocimientos de los miembros la compañía sobre el uso de las TIC?	x			1	1	
		6	¿Los miembros de la compañía son independientes a la administración y por tanto sus decisiones son libres y objetivas?		x		1	0	
	Principio 3. La Gerencia Establece estructura, autoridad, y responsabilidad	7	¿La estructura organizativa y funcional permite el cumplimiento de sus objetivos?	x			1	1	
		8	¿La compañía cuenta con especialistas con conocimientos sobre las TI sea internos o externos?	x			1	1	
		9	¿En el desarrollo de estrategias del departamento consideran la inversión y uso de las TI?	x			1	1	
		10	¿Se modifica de forma constante la estructura, funciones y responsabilidades en la compañía?	x			1	1	
	Principio 4. La organización demuestra compromiso por reclutar y mantener colaboradores competentes.	11	¿ La empresa tiene un proceso definido para el reclutamiento de nuevos empleados, según los requerimientos departamentales?	x			1	1	
		12	¿La empresa mantiene comunicación directa con los empleados enfatizando sus responsabilidades y lo que la dirección espera de ellos?	x			1	1	
		13	¿Se formula un plan de capacitación para el personal de la compañía?	x			1	1	
		14	¿Se socializa el plan de capacitación al personal de la compañía?	x			1	1	
	Principio 5. Hace cumplir con la responsabilidad	15	¿Se realiza un reconocimiento a los colaboradores que se destaquen en el cumplimiento de las normas éticas, así como en el desempeño esperado?	x			1	1	
		16	¿Los empleados son conscientes del compromiso laboral con la empresa considerando que de existir un comportamiento no aceptable o incumplimiento a las normas internas son motivo de sanciones?	x			1	1	
			TOTAL				**16**	**15**	
EVALUACIÓN DE RIESGOS	**Principio 6. La organización define objetivos claros y relevantes, que permiten la identificación y evaluación de riesgos asociados.**	1	¿ Los objetivos establecidos están alineados con la estrategia de la compañía y con las normas internas y externas que la regulan?	x			1	1	
		2	¿Se ha definido procedimientos claves para la identificación de vulnerabilidades en sus activos de información?	x			1	1	

	Principio 7. Se identifican y analizan los riesgos para el logro de los objetivos.	3	¿Los directivos de la compañía identifican los riesgos que pueden afectar el logro de los objetivos institucionales, en base a los factores internos o externos?	x			1	1	
		4	¿Se conocen los controles que la compañía aplica relacionados con los riesgos identificados?	x			1	1	
		5	¿La compañía cuenta con un sistema de seguridad y vigilancia para la prevención de amenazas que puedan atentar a la integridad de su personal?	x			1	1	
	Principio 8. Se evalúa el riesgo de Fraude	6	¿Tienen mecanismos adecuados para identificar riesgos internos?	x			1	1	
		7	¿Se consideran diferentes riesgos de fraude, tal como la corrupción y la pérdida de activos de información, en el análisis de riesgos de la compañía?	x			1	1	
		8	¿Se evalúa los riesgos por ataques cibernéticos?	x			1	1	
		9	¿El departamento ha sufrido fraude o robo de información por parte de un colaborador interno?	x			1	1	
	Principio 9. Se identifican y analizan cambios importantes que puedan impactar el Sistema de Control Interno	10	¿Se realiza un seguimiento del impacto que podrían tener la materialización de los riesgos sobre los objetivos del departamento?		x		1	0	
		11	¿Se consideran criterios importantes de evaluación a recursos humanos, presupuesto, sistemas de información diseño de procesos, claves de seguridad, respaldos, mantenimiento y la seguridad, integridad y autenticidad de datos?	x			1	1	
		12	¿La empresa realiza comprobación periódica de la seguridad, integridad y autenticidad de datos?	x			1	1	
			TOTAL				**12**	**11**	
ACTIVIDADES DE CONTROL	**Principio 10. Seleccionar y Desarrollar Actividades de Control**	1	¿Las actividades de control aplicados en la empresa son tanto preventivos como correctivas?	x			1	1	
		2	¿Tienen manuales, instructivos o normas de forma escrita que regulen el desarrollo de las diferentes actividades de trabajo con el uso de las TIC?	x			1	1	
		3	¿La compañía tiene instaladas cámaras de seguridad como procedimiento de control preventivo ante cualquier anomalía en sus instalaciones?	x			1	1	
	Principio 11. La organización selecciona y	4	¿Se han implementado controles orientados sobre el desarrollo, compra y mantenimiento de programas e infraestructura de TI?	x			1	1	
		5	¿Se asegura lógica y físicamente los equipos e infraestructura de TI?	x			1	1	

	desarrolla controles generales sobre tecnología	6	¿ Se utilizan mecanismos de control para el acceso y autenticación de usuarios no autorizados?	x			1	1	
		7	¿Se ha implementado un software antivirus?	x			1	1	
		8	¿Se realiza mantenimiento periódico al software antivirus?	x			1	1	
		9	¿Se define perfiles y permisos de usuario en cada una de las herramientas de apoyo tecnológico de acuerdo con el rol desempeñado?	x			1	1	
		10	¿Se han implementado controles orientados a la adquisición y mantenimiento de los activos de información?	x			1	1	
	Principio 12. Implementación de las actividades de control, por medio de políticas y procedimientos.	11	¿Los responsables de cada departamento diseñan controles relacionados con planes y programas de la actividad que desarrolla?	x			1	1	
		12	¿Se ha dado seguimiento a la rotación de tareas, de manera que tenga independencia, separación de funciones incompatibles?	x			1	1	
			TOTAL				**12**	**12**	
INFORMACIÓN Y COMUNICACIÓN	**Principio 13. Generar y utilizar información relevante y de calidad.**	1	¿Se identifica y presenta con seguridad la información, generada dentro de la compañía, esencial para el logro de los objetivos de la compañía?	x			1	1	
		2	¿La calidad y oportunidad de la información permite la toma de decisiones adecuada, tanto hacia la máxima autoridad como a los jefes de los departamentos?	x			1	1	
		3	¿Existe la suficiente comunicación que facilite al personal de la compañía a cumplir sus funciones?	x			1	1	
	Principio 14. Información Interna	4	¿En el departamento se ha definido los métodos de comunicación que son válidos en cada uno de los procesos, tales como correos electrónicos, memorandos internos, comités, intranet y mensajes de texto, entre otros?	x			1	1	
		5	¿La información se facilita con el detalle adecuado para los distintos niveles de gestión?	x			1	1	
		6	¿Tienen un protocolo para la comunicación de información a los niveles superiores de la compañía?	x			1	1	
		7	¿Se realizan acciones de seguimiento, que permitan validar el cumplimiento de los objetivos de la organización?	x			1	1	

	Principio 15. Comunicación Externa o a terceros	8	¿Se han definido los responsables de la recepción de información de los entes externos, reduciendo la posibilidad de no atender un requerimiento por falta de gestión o conocimiento al interior de la organización?	x			1	1	
			TOTAL				**8**	**8**	
SEGUIMIENTO Y MONITOREO	**Principio 16. Evaluaciones Continuas o Independientes**	1	¿Se realizan evaluaciones de seguimiento continuo sobre las actividades, que cada una de las unidades realiza, y que permitan aplicar medidas oportunas?	x			1	1	
		2	¿Existen procedimientos para que la dirección revise los procesos de control de las TIC, para asegurarse de su cumplimiento del modo esperado?	x			1	1	
	Principio 17. Evaluación y comunicación de las deficiencias encontradas.	3	¿Los resultados de las evaluaciones realizadas, bien sea independientes o continuas son revisadas por los directivos o la Gerencia?	x			1	1	
		4	¿La empresa realiza un seguimiento frecuente a las deficiencias encontradas en procesos internos que afecten al desarrollo normal de sus actividades?	x			1	1	
		5	¿Se aplica procedimientos para la mejora continua de las actividades internas?	x			1	1	
			TOTAL				**5**	**5**	
			TOTAL GENERAL				**53**	**51**	

Anexo 4. Modelo de matriz de seguimiento de controles de las TIC

	**Matriz de verificación del cumplimiento de Controles de las TIC**

N°	Control	Objetivo	Descripción	Responsable	Fecha de aplicación	Efectividad	Observación

Elaborado por…… **Aprobado por…….**

Revisado por……. **Fecha de aprobación.....**

Anexo 5. Matriz de seguimiento de recomendaciones del informe

GRUPO IMPACTEX	**Matriz de monitoreo y seguimiento de recomendaciones**

N°	Recomendación	Responsable	Temporalidad	Acción	Fecha de aplicación	Resultado	Observación
1	Mantener los soportes informáticos en un lugar cerrado al momento en que no sean utilizados, además aplicar un control de bloqueo de pantallas y designación de contraseñas para proteger los equipos que se encuentran sin vigilancia.	dpto. de sistemas	1 semana				
2	Implementar una política sobre la seguridad de la información en la que se establezca los tipos de controles a aplicar tales como preventivos, detectivos y correctivos.	Jefe de sistemas	1 semana				
3	Asignar personal para que se encargue de la evaluación periódica de los departamentos de marketing y financiero.	Gerente de la compañía	2 días				
4	Elaborar un cronograma de capacitación para cada departamento con horarios dentro de la jornada laboral.	Jefe de Talento Humano	2 días				
5	Especificar las responsabilidad de cada empleado y los objetivos a alcanzar al momento de incorporar a un empleado en su departamento.	Jefe de marketing	En la inducción del personal				
6	Supervisar que el personal a cargo realice las actividades según sus perfiles en cada una de sus tareas.	Jefe de sistemas	Mensual				
7	Desarrollar un mapa de riesgos con escalas que identifiquen el impacto de los mismos, además, del seguimiento periódico por sus consecuencias.	Jefe de finanzas y sistemas	1 semana				

8	Supervisar el cumplimiento de quienes están a cargo de monitorear amenazas y vulnerabilidades en los activos de información.	Jefe de marketing	Cada 15 días				
9	Diseñar indicadores internos que permitan evaluar la eficiencia, el desempeño y la eficacia de las actividades y resultados sobre el cumplimiento de sus objetivos departamentales.	Jefe de sistemas	2 semanas				
10	Asignar a un responsable para gestionar los procesos y periodos de revisión de controles que están aplicando dentro del departamento de finanzas para un mejor y adecuado gobierno y gestión de las TIC.	Jefe de sistemas	1 semana				

Elaborado por…… **Aprobado por…….**

Revisado por…… **Fecha de aprobación.....**