



TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Auditoria con la Norma ISO 20000
para la Medición de la calidad de
Procesos TI en la Empresa Maikai
Tec. S.A. de C.V.

Reporte Final de Residencias
Profesionales

INGENIERÍA EN SISTEMAS COMPUTACIONALES

Especialidad
Auditoría en Seguridad Informática

Presenta:

Alan Manuel Sánchez Fuentes

Calificación: _____

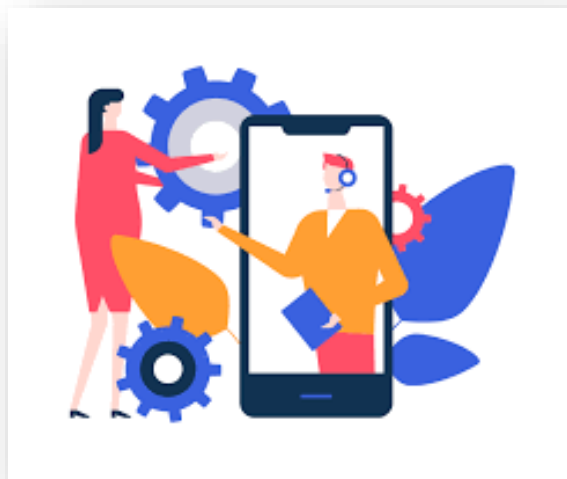
Coacalco de Berriozábal, Febrero/ 2023

AGRADECIMIENTOS

Quiero dedicar este trabajo a mi madre, la señora Julieta Fuentes, que con su apoyo incondicional he llegado a convertirme en el hombre que soy ahora. Gracias por alentarme en aquellos momentos de duda e incertidumbre en donde con unas simples palabras me motiva a continuar y no rendirme fácilmente. Jamás podré agradecerle lo suficiente, gracias por haber sido mi soporte durante tantos años. La principal persona que me apoyo siempre fue ella.

RESUMEN

La finalidad del proyecto de auditoria basada en una norma ISO (20,000) parte de una problemática al tener una empresa que no cuenta con un plan o ciclo de vida de sus procesos teniendo la necesidad de establecer estrategias para definirlos y medir su nivel de calidad de servicios de TI. La norma será enfocada a la medición de calidad de los servicios que la empresa brindé para esto debemos enfocarnos en parámetros y esquemas de trabajo ordenados para saber que vamos a preguntar, como vamos a abordar la situación y que áreas de acción tendremos, con el fin de tener un catálogo de propuestas para poder dar solución de manera retroactiva a la empresa auditada. Con estas soluciones pretendemos ver una mejoría en su nivel de respuesta a aquellos problemas que la empresa enfrenta con cotidianidad y por ende tener una oportunidad de optimización continua.



ÍNDICE

Capítulo 1. Generalidades del Proyecto	8
1.1 Introducción	9
1.2 Descripción de la Empresa	10
1.2.1 Nombre o Razón Social	10
1.2.2 Ubicación	10
1.2.3 Organigrama	10
1.2.4 Sector Productivo de la Empresa	10
1.2.5 Misión, Visión Y/O Valores de la Empresa	10
1.2.5.1 Misión	10
1.2.5.2 Visión	11
1.2.5.3 Valores	11
1.2.6 Calidad	11
1.2.7 Orientación al Cliente	11
1.2.8 Resolución de Problemas	11
1.2.9 Breve Historia de la Empresa	12
1.3 Problema a Resolver	13
1.4 Objetivos	14
1.5 Justificación	16
Capítulo 2. Marco Teórico	17
2.1 Marco Histórico	18
2.1.1 La ingeniería en Sistemas Computacionales.	18
2.1.2 Ciclo de vida del periodo de la ingeniería.....	18
2.1.3 La informática	18
2.1.4 La Digitalización	19
2.1.5 Digitalización de Procesos	19
2.1.6 Tecnologías de la Información	20
2.1.7 Perfil Profesional Para La Implementación Y Administración De Las TI (Tecnologías De La Información)	20
2.1.8 Enfoque Informático En El Mundo Empresarial	21

2.1.9	La auditoría	21
2.1.10	Normalización	24
2.1.11	Normas	25
2.1.12	Acerca De Las Normas ISO	26
2.1.13	Ventajas De Las Normas ISO Ante Sociedad Y Mercados	27
2.1.14	ISO 20000	27
2.1.15	TI En México	28
2.2	Marco Conceptual	28
2.2.1	La Ingeniería En Sistemas Computacionales	29
2.2.2	La Informática	29
2.2.3	La Digitalización	29
2.2.4	Digitalización de Procesos	29
2.2.5	Tecnologías de la Información	30
2.2.6	La Auditoria	30
2.2.7	La Auditoría Informática	30
2.2.8	Normas	30
2.2.9	Normalización	30
2.2.10	Normas ISO	31
2.3	Marco Metodológico	31
Capítulo 3. Desarrollo y Resultados		33
3.1	Objetivo 1. Reconocer	34
3.1.1	Visitar el área de trabajo	34
3.1.2	Estudio preliminar de los servicios y procesos de TI	38
3.1.3	Políticas de Confidencialidad / Recolección de Datos	39
3.1.4	Matriz Diagnóstica – Prioridades y Riesgos	39
3.1.5	Formulario de Evaluación del Riesgo	41
3.2	Objetivo 2. Investigar	43
3.2.1	Formular el plan de auditoría.....	44
3.2.2	Reconocer bases de la norma ISO 20000.....	44
3.2.3	Elaboración de solicitud de auditoría.....	45

3.2.4	Elaboración de cuestionarios y rubros apegados al modelo de ISO 20000	51
3.2.5	Elaboración de entrevistas y rubros apegados al modelo ISO 20000	51
3.2.6	Cuestionarios de procesos COBIT	55
3.2.7	Evaluación de los resultados de los cuestionarios	55
3.3	Objetivo 3. Presentar	58
3.3.1	Informe de auditoría	58
Capítulo 4.	Conclusiones.....	69
Capítulo 5.	Competencias Desarrolladas	70
Capítulo 6.	Fuentes de Información	71

ÍNDICE DE FIGURAS

Organigrama Maikai Tec	10
Tabla 1 “Matriz de Diagnostico – Prioridades y Riesgos”	40
Tabla 2 “Matriz de Diagnostico – Prioridades y Riesgos”	43
Figura 1. Proceso ISO 20000	46
Figura 2. Metodología para la mejora de procesos TI	47
Figura 3. Metodología para la implantación de los procesos de la norma ISO 20000	48
Figura 4. Acciones para la mejora de procesos	50
Tabla 3. Entrevista acerca de los procesos y servicios TI	52
Tabla 4. Matriz de Evaluación de Dominio de Procesos COBIT	56
Tabla 5. Resultado Porcentajes de Matriz de Evaluación COBIT	57
Figura 5. Gráfica de Resultados Entrevista	58
Tabla 6. Tabla General del Dominio de Planificación y Organización	60
Figura 6. Gráfica de Resultados Tabla General del Dominio de Planificación y Organización.	60
Tabla 7. Tabla General del Dominio de Adquisición e Implementación.	62
Figura 7. Gráfica de Resultados Tabla General del Dominio de Adquisición e Implementación.	62
Tabla 8. Tabla General del Dominio de Entrega y Soporte.	63
Figura 8. Gráfica de Resultados Tabla General del Dominio de Entrega y Soporte	64
Tabla 9. Indicador Tabla General del Dominio de Planificación y Organización	65
Tabla 10. Indicador Tabla General del Dominio de Adquisición e Implementación	65
Tabla 11. Indicador Tabla General del Dominio de Entrega y Soporte	65
Tabla 12. Niveles de Madurez CMMI	65
Tabla 13. Hallazgos y Recomendaciones	66

CAPÍTULO I

GENERALIDADES DEL PROYECTO

INTRODUCCIÓN

Generalidades de la auditoría en base a la norma ISO / IEC 20000

El presente proyecto tiene un objeto de investigación, estudio, análisis, y aplicación de la auditoría la cual basa los mismos principios mencionados en la norma ISO 20000. La auditoría siendo una herramienta que pretende ayudar de manera cuantitativa y cualitativa los procesos, activos y recursos sobre los que giran los servicios de una empresa de un área determinada delimitando las capacidades, amenazas a las que se enfrenta y oportunidades a las que aspira. Este enfoque lo brindará la auditoría la cual debe estar fundamentada de manera ordenada en un esquema de trabajo donde podamos establecer los pasos iniciales definidos en procesos que nos ayuden a trazar el camino para realizar la auditoría con las herramientas pertinentes y de esta manera poder obtener el alcance de la norma.

La aplicación de la auditoría puede ser un factor a favor de una empresa, pero también puede verse enfrentada a la resistencia por naturaleza de los procesos que están determinados en el tiempo y espacio del área designada, así como la totalidad de la norma que puede ser delimitada por la accesibilidad en un enfoque educativo como lo es el presente proyecto.

Para darle solución a esta limitante se realiza un análisis en base a los objetivos y podemos determinar una planeación donde el proyecto tendrá un inicio, un desarrollo y un final. Se tendrá que establecer tres fases de estudio, análisis y planteamiento donde podremos tener fundamentos teóricos y metodológicos para sustentar los procesos y herramientas de auditoría.

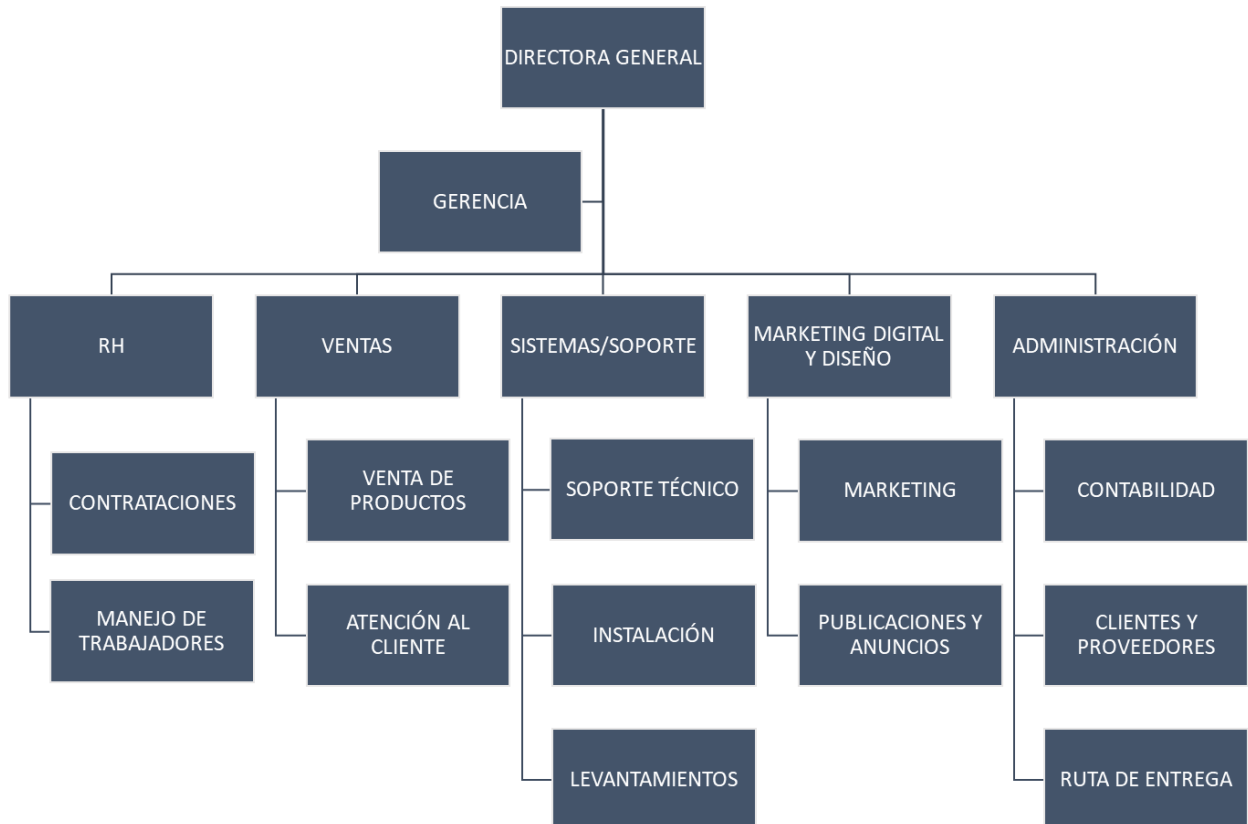
Finalmente comprender la interpretación y la presentación del informe de auditoría, concluyendo en aquellas propuestas que sean atractivas para la empresa auditada teniendo como aspiración un nivel de madurez optimo y definido aparte de tener un cimiento para la certificación ISO/IEC 20,000.

DESCRIPCIÓN DE LA EMPRESA

1.2.1 Nombre o Razón Social: Maikai Tec. S.A. de C.V.

1.2.2 Ubicación: Av. José Lopez Portillo No. 206 planta baja, Col. Zacuautitla, Coacalco Estado de México, C.P. 55700

1.2.3 Organigrama



Organigrama Mai Kai Tec. S.A de C.V

1.2.4 Sector Productivo de la Empresa: Comercial, Terciario

1.2.5 Misión, Visión y Valores.

1.2.3.1 Misión.

Ser una empresa innovadora que busca el máximo beneficio de nuestros clientes a través de la calidad de nuestras soluciones, productos y servicios, manteniendo las mejores condiciones de trabajo para nuestros colaboradores.

1.2.3.2 Visión

Las nuevas tecnologías están cambiando el modo en que pensamos, nos comunicamos y hacemos negocios, Maikai Tec quiere contribuir en la aplicación de estas tecnologías en tu empresa y continuar innovando de la mano de su comunidad de clientes, proveedores y empleados. Esto nos permitirá seguir creciendo de manera constante, para afianzarnos como un referente en el sector, con una fuerte presencia nacional y diversificando la actividad hacia otras áreas emergentes donde pongamos en valor nuestros conocimientos y experiencia.

1.2.3.3 Valores

Una empresa 100% mexicana con más de 30 años de experiencia en el ramo de tecnología y servicios de TI, dedicada a resolver necesidades de los clientes con servicios y productos tecnológicos. Entusiasta por la tecnología, ayudando a crecer a un servidor, mejorando así el entorno tecnológico de las personas.

1.2.6 Calidad

Vivimos en un mundo donde todos dicen que tienen los mejores productos del mercado. Pero una cosa es afirmarlo y la otra es garantizarlo. Por consiguiente, en lo que ofrecemos a los clientes, es lo que aseguramos.

1.2.7 Orientación al cliente

Tratamos de satisfacer por completo cada una de las peticiones y/o necesidades, en cada uno de nuestros productos y servicios, mediante un trato digno y totalmente cordial. El cliente, como parte de nuestro eje central.

1.2.8 Resolución de problemas

Para todos nuestros consumidores, así como de nuestros usuarios, el valor de la resolución de problemas es tan importante, ya que gracias a ellos crecemos y mejoramos cada día, para poder brindar un mejor servicio sin ningún problema.

1.2.9 Breve historia de la empresa.

Claudia Vázquez, quién actualmente lleva 30 o más años en el mercado, comenzó trabajando como vendedora de artículos y productos de TI, trabajando para otras personas, renuncia y decide poner su propia empresa para sacar a sus hijas adelante siendo madre soltera y sin depender de nadie.

Con la experiencia y los clientes con los que ya contaba, emprendió como persona física y con su amplia cartera que tiene, empezó poco a poco hasta convertirse en persona moral y poder expandirse a las corporativas, con el denominado nombre “Maikai Tec”.

1.3 PROBLEMA A RESOLVER

Cada vez es mayor el número de empresas que ofrece servicios TI, por lo que la competencia también aumenta. Cuando un cliente contrata a una empresa de servicios TI, el hecho de ver que dispone de la certificación ISO 20000 le garantiza que va a recibir unos servicios de calidad que siguen las mejores prácticas reconocidas a nivel internacional. Por lo que dentro de la empresa Maikai Tec se busca mejorar la calidad de los procesos implementados. La norma será enfocada a la medición de calidad de los servicios que la empresa brindé para esto debemos enfocarnos en parámetros y esquemas de trabajo ordenados para saber cómo vamos a abordar la situación y que áreas de acción tendremos, con el fin de tener un catálogo de propuestas para poder dar solución de manera retroactiva a la empresa auditada

Una vez concluyendo con este proyecto se esperan los siguientes beneficios:

- Mejorar la reputación.
- Aumentar la productividad.
- Garantiza cumplir con el nivel exigido.
- Dinamismo y rapidez, así como la habilidad y la velocidad con los procesos que se realizan.
- Ventajas ante la competencia.



1.4 OBJETIVOS

1.5.1 OBJETIVO GENERAL

Garantizar que la metodología y buenas prácticas están correctamente establecidas en los procesos realizados por la empresa, basándose en la norma ISO 20000, dentro de la empresa Maikai Tec.

1.5.2 OBJETIVOS ESPECIFICOS

ESP 1.0 Reconocer.

Reconocer el área con la ayuda de los encargados (ingenieros, técnicos, licenciados) del departamento de sistemas, para definir los procesos que serán auditados, con el fin de poder analizarlos según la norma ISO 20,000.

- 1.1 Visitar el área de trabajo.
- 1.2 Estudio preliminar de los servicios y procesos de TI.
- 1.3 Selección de los procesos para auditar / Elaboración de cuestionarios de preauditoria.
- 1.4 Políticas de Confidencialidad / Recolección de Datos.
- 1.5 Matriz Diagnóstica – Prioridades y Riesgos.
- 1.6 Formulario de Evaluación del Riesgo

ESP 2.0 Investigar

Investigar qué puntos establece la norma ISO 20000 haciendo el uso de artículos, documentación, webinar etc. y basar un plan de acción en base a su implementación para adaptar el proceso de auditoría.

- 2.1 Formular el plan de auditoría.
- 2.2 Reconocer bases de la norma ISO 20000.
- 2.3 Elaboración de solicitud de auditoría.
- 2.4 Elaboración de cuestionarios y rubros apegados al modelo de ISO 20000.
- 2.5 Elaboración de entrevistas y rubros apegados al modelo ISO 20000

2.6 Cuestionarios de procesos COBIT.

2.7 Evaluación de los resultados de los cuestionarios.

ESP 3.0 Presentar

Representación de los resultados obtenidos mediante la documentación y recursos gráficos a los encargados del departamento de sistemas para fundamentar el nivel y recomendaciones para el área auditada.

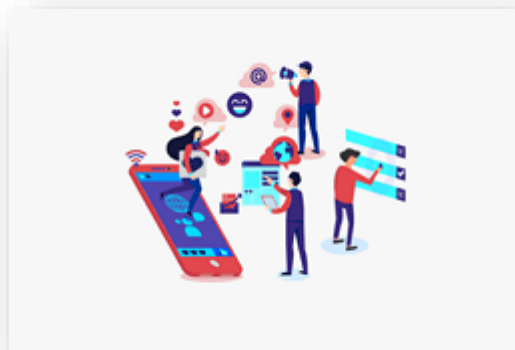
3.1 Informe de Auditoría.

JUSTIFICACIÓN

El presente proyecto encuentra su justificación en el empleo de la investigación, técnicas, herramientas y conocimientos aplicados en el desarrollo de una auditoría externa, contemplando aquellas competencias dictaminadas en el plan de estudios de la especialidad de auditoría en la seguridad informática transportando los conocimientos esperados a una situación práctica donde se pueda evaluar los procesos de una empresa apoyándose y haciendo uso de una norma ISO (ISO / IEC 20,000) para medir su calidad del servicio de TI.

El interés personal y académico sobre este proyecto se basa en la necesidad de comprobar el impacto de una auditoría y obtener mejoras estableciendo estadísticas y analizando los resultados de manera correcta; una vez teniendo los resultados hacer de ellos un catálogo de propuestas que puedan ser atractivas para la empresa auditada y así tener una aspiración a una certificación en la norma ISO aplicada.

Las buenas prácticas están ligadas a una correcta preparación de una actividad, convirtiéndose en un ciclo vicioso con el que las ejecuta ayudando a una empresa a un enfoque objetivo dentro de una meta a largo plazo (que sea escalable) lo que genera confianza para perfilarse en una empresa líder o considerarla como una empresa seria debido a su nivel de preparación.



CAPÍTULO II

MARCO TEÓRICO

2.1 Marco Histórico

Para poder comprender los marcos teóricos que aborda el presente proyecto, debemos partir de las incógnitas conceptuales, así como entrar en el contexto histórico y plantar nuestro presente como las situaciones a las que enfrenta la constante evolución de los sistemas.

2.1.1 La Ingeniería En Sistemas Computacionales

La ingeniería de sistemas se encarga del diseño, la programación, la implantación y el mantenimiento de sistemas. A diferencia de otras ramas de la ingeniería, esta disciplina no se ocupa de productos tangibles (los ingenieros civiles, por ejemplo, construyen edificios), sino de productos lógicos. Por lo tanto, la ingeniería de sistemas implica el uso de nociones matemáticas que permitan concretar la aplicación tecnológica de las teorías de los sistemas. Se trata de una ciencia interdisciplinaria, que requiere de diversos conocimientos para plasmar sus diseños en la vida práctica. La ingeniería de sistemas permite transformar una necesidad operativa en una descripción de los parámetros del rendimiento de un sistema, con su correspondiente configuración. Por otra parte, posibilita la integración de los parámetros técnicos relacionados de modo tal que las interfaces de programa y funcionales sean compatibles y se garantice el funcionamiento del sistema total.

De la misma forma, la ingeniería de sistemas también está íntimamente relacionada con la investigación de operaciones y con los llamados sistemas de información, es decir, los elementos que funcionan y trabajan juntamente con el claro objetivo de poder ayudar a las tareas y actividades de una empresa. Más concretamente contribuyen a respaldar dichas acciones a través de lo que es la entrada, el almacenamiento, el procesado y la posterior salida de la información.

2.1.2 Ciclo De Vida Del Producto De La Ingeniería

Al realizar su trabajo, el especialista en esta materia debe asegurar que el sistema cumpla con los principios de fiabilidad, mantenibilidad, seguridad y eficiencia, entre otros.

2.1.3 La Informática

La informática se refiere al procesamiento automático de información mediante dispositivos electrónicos y sistemas computacionales. Los sistemas informáticos deben contar con la capacidad de cumplir tres tareas básicas: entrada (captación de la información),

procesamiento y salida (transmisión de los resultados). El conjunto de estas tres tareas se conoce como algoritmo. La informática reúne a muchas de las técnicas que el hombre ha desarrollado con el objetivo de potenciar sus capacidades de pensamiento, memoria y comunicación. Su área de aplicación no tiene límites: la informática se utiliza en la gestión de negocios, en el almacenamiento de información, en el control de procesos, en las comunicaciones, en los transportes, en la medicina y en muchos otros sectores.

Con el tiempo los sistemas de información han evolucionado a tal manera de ser la representación actual de la vida en el mundo digital. Las empresas y la información, así como los métodos de almacenamiento dónde podemos tener volúmenes gigantes de información en espacios pequeños y el procesamiento de esta información a velocidades récord coloca a la informática como un pilar para todas las grandes, medianas, y pequeñas empresas para dar solución a las actividades cotidianas y mantener un patrimonio tecnológico que se adecue a las nuevas modalidades económicas, publicitarias o de entretenimiento que se refieren en la actualidad.

2.1.4 La Digitalización

La digitalización es un proceso mediante el cual, algo real (físico, tangible) es pasado a datos digitales para que pueda ser manejado por una computadora (de naturaleza, a su vez, digital), modelándolo, modificándolo, y aprovechándolo para otros propósitos distintos de su cometido o función originales.

Las nuevas soluciones digitales tienen el hábito de desplazar a sus contrapartes más antiguas y, cuando esas soluciones llegan, la adopción es mucho más fácil si ya estás actualizado. Considera lo fácil que fue la transición que realizaste desde los CD a la transmisión de música. Al principio, nos permitíamos usar las dos modalidades, ya que las PC y los estéreo de los coches ofrecían una transición suave con los reproductores de CD y los conectores de entrada auxiliar. Ahora, debes realizar un gran esfuerzo para conseguir un reproductor de CD, mientras que tienes un reproductor de MP3 integrado a tu teléfono, así como lector de libros electrónicos y monitores de actividad.

2.1.5 Digitalización de Procesos

La digitalización de procesos en la mayoría de los casos en los negocios se refiere a mejorar los procesos, las funciones y operaciones comerciales mediante el aprovechamiento de la nueva tecnología que proporciona el espacio digital.

En promedio, la digitalización en este sentido de la palabra se considera el paso intermedio hacia la transformación digital y la creación de flujos de ingresos digitales.

2.1.6 Tecnologías De La Información (TI)

La noción abarca cuestiones propias de la informática, la electrónica y las telecomunicaciones. A pesar de que el concepto de tecnología de la información se considera idéntico a los conceptos de computadora y red informática, el uso del concepto de TI en sí no puede limitarse a las computadoras. Las herramientas de tecnología de la información son un tipo de tecnología informática con la que se busca, procesa y transmite la información.

Las herramientas informáticas son de tres tipos:

- Computacional: dispositivos automatizados para recoger y procesar información
- Organizacional: diferentes tipos de equipos para realizar tareas técnicas
- Comunicación de equipos: laptops, computadoras, teléfonos inteligentes, tabletas y otros dispositivos.

La persona promedio emplea sólo dispositivos de comunicación en la vida cotidiana. Los dispositivos informáticos y organizativos están diseñados para que los profesionales de la informática resuelvan tareas importantes.

Se cree que la informática comenzó a desarrollarse tras la llegada de los ordenadores. Pero en realidad su historia se remonta a los tiempos primitivos, cuando la gente compartía datos mediante dibujos rupestres.

2.1.7 Perfil Profesional Para La Implementación Y Administración De Las TI (Tecnologías De La Información)

Se espera que un profesional de este campo haya adquirido los conocimientos necesarios para diseñar, desarrollar, aplicar y mantener sistemas computacionales de información, además de ser capaz de brindar soporte a los demás empleados de la compañía en la que se desempeña. Se trata de un rol complementario, por ejemplo, al de los programadores, ya que

tiene a su cargo la instalación y el mantenimiento de todos los programas usados en la empresa, la administración y reparación de las redes y la actualización de los dispositivos.

2.1.8 Enfoque Informático En El Mundo Empresarial

La mayoría de las empresas de la actualidad hacen uso de la tecnología de la información de manera constante. Tomemos el caso de una tienda de ropa que cuenta con un sitio web donde presenta datos de sus productos y, además, utiliza el correo electrónico para contactarse con sus clientes y proveedores. En el local, una computadora permite registrar las operaciones y emitir las facturas que entregan a los compradores. En la computadora además se registran los movimientos de stock.

Muchas personas también apelan a la tecnología de la información en la vida cotidiana, comunicándose por correo electrónico, chat o teléfono; viendo televisión para informarse; y utilizando consolas de videojuegos como entretenimiento, por citar apenas algunas actividades.

Resumen

Entendiendo la relación que hay entre los conceptos y paradigmas mencionados, podemos resumir que el perfil del ingeniero en sistemas debe entender su papel dentro de una empresa, de un equipo de trabajo, ante la sociedad y en la búsqueda de respuestas de un supuesto. El medio ambiente que desenvuelve al ingeniero por naturaleza lo relaciona con la informática siendo está un área que de la mano de la tecnología buscan la aceleración de procesos en el mundo digital, las soluciones y las optimizaciones para poder dar pie a la innovación y creación de más tecnologías que ayuden a un enfoque futurista y progresista.

Teniendo esto en cuenta podemos interpretar la creación de la ingeniería como un hecho que necesite una comprobación y validación de ciertos parámetros para poder cumplir su voluntad ante el enfoque mencionado.

2.1.9 La auditoria

Antecedentes

Se sabe qué hace varios siglos ya se practicaban auditorías. Muchos reyes o gente poderosa tenían como exigencia la correcta administración de las cuentas por parte de los escribanos, de modo que se pudieran evitar desfalcos o que alguna persona se aprovechara de las riquezas que en aquella época costaban tanto sudor y sangre conseguir.

Sin embargo, los antecedentes de la auditoría, los encontramos en el siglo XIX, por el año 1862 donde aparece por primera vez la profesión de auditor o de desarrollo de auditoría bajo la supervisión de la ley británica de Sociedades anónimas. Para evitar todo tipo de fraude en las cuentas, era necesario una correcta inspección de las cuentas por parte de personas especializadas y ajenas al proceso, que garantizaran los resultados sin sumarse o participar en el desfalco.

Desde entonces, y hasta principios del siglo XX, la profesión de auditoría fue creciendo y su demanda se extendió por toda Inglaterra, llegando a Estados Unidos, donde los antecedentes de las auditorías actuales fueron forjándose, en busca de nuevos objetivos donde la detección y la prevención del fraude pasaba a segundo plano y perdía cierta importancia.

En los años cuarenta empezaron a darse resultados relevantes en el campo de la computación, con sistemas de apoyo para estrategias militares entre otros, posteriormente se vino incrementando el uso de las computadoras y sus aplicaciones. Se diversificó el apoyo a otros sectores de la sociedad: Educación, Salud, Industrial, Político, Banca, Aeronáutica, Comercio, Etc.

En aquellos años la seguridad y control de ese medio ambiente se limitaba a dar custodia física a los equipos y a permitir el uso de estos por personal altamente calificado (no había un gran número de usuarios ya sea técnicos o administrativos).

Actualmente el medio ambiente de la Informática se ha extendido a todas las ramas de la sociedad, es tan factible controlar un vuelo espacial por medio de una computadora, como seleccionar las compras del hogar desde una microcomputadora.

Objetivo de una auditoría

El objetivo fundamental de un trabajo de auditoría es permitir que el auditor llegue a estar en condiciones de informar fundamentalmente sobre la fidelidad y razonabilidad de la situación que refleja la documentación aportada por la empresa. El auditor está obligado a establecer de forma inequívoca, según su criterio, si la imagen de la empresa es fiel y

razonable en la documentación aportada. Si no ha podido confirmar estos términos, debe calificar su informe justificando las razones que le han llevado a considerar las desviaciones de fidelidad y razonabilidad, y en qué aspectos, y en qué medida, se ha incurrido en una formulación errónea. El auditor debe expresar con independencia su opinión.

Existen dos tipos de auditoría:

- La auditoría interna. La auditoría interna es un proceso independiente y objetivo diseñado para aportar valor a una empresa a través del análisis y evaluación de la eficacia de sus procesos de gestión de riesgos, control y gobierno.
- La auditoría externa. La auditoría externa es una práctica común en empresas e instituciones, donde profesionales auditores procedentes del exterior evalúan que una empresa funciona correctamente en relación con los procesos que asume y su marco normativo.

Conclusión de una auditoría

La auditoría intenta también brindar pautas que ayuden a los miembros de una empresa a desarrollar adecuadamente sus actividades, evaluándolos, recomendándoles determinadas cosas y revisando detenidamente la labor que cada uno cumple dentro de la organización.

La Auditoría Informática

La auditoría informática se desarrolla en base a normas, procedimientos y técnicas definidas formalmente por Institutos establecidos a nivel nacional e internacional.

Prof. Dr. José Miguel Castillo (2016) Menciona mediante una clase magistral que la práctica de validación como necesidad de un control es lo que comprende la actividad de una auditoría informática. La auditoría informática debe hacer énfasis en el área de desarrollo y seguridad, así como auditar el correcto seguimiento de normas y metodologías para poder ser candidatos a una certificación.

Siempre ha existido la preocupación por parte de las organizaciones por optimizar todos los recursos con que cuenta la entidad, sin embargo, por lo que respecta a la tecnología de informática, es decir, software, hardware, sistemas de información, investigación tecnológica, redes locales, bases de datos, ingeniería de software, telecomunicaciones, etc. esta representa una herramienta estratégica que representa rentabilidad y ventaja competitiva

frente a sus similares en el mercado, en el ámbito de los sistemas de información y tecnología un alto porcentaje de las empresas tiene problemas en el manejo y control, tanto de los datos como de los elementos que almacena, procesa y distribuye.

Las áreas para auditar en donde se puede realizar la auditoría en informática pueden ser:

- A toda la entidad.
- A un departamento.
- A un área.
- A una función.
- A una subfunción.

Y se pueden aplicar los siguientes tipos de auditoría:

- Auditoría al ciclo de vida del desarrollo de un sistema.
- Auditoría a un sistema en operación.
- Auditoría a controles generales (gestión).
- Auditoría a la administración de la función de informática.
- Auditoría a microcomputadoras aisladas.
- Auditoría a redes.

Algunos de los puntos que comprende la auditoria informática son:

- El control de la función informática.
- El análisis de la eficacia del sistema informático.
- La verificación de la implantación de la normativa.
- La revisión de la gestión de los recursos informáticos.

2.1.10 Normalización

Permite la creación de normas o estándares que establecen las características comunes que deben cumplir los productos en diferentes partes del mundo. Esto significa que su manufactura o fabricación debe ser de la misma forma en México, Estados Unidos, China, o en cualquier otro país o parte del mundo.

Es, además, una actividad técnica especializada que ofrece muchos beneficios a nuestra sociedad: permite que las pequeñas y medianas empresas puedan acceder a mercados internacionales; contribuye a la reducción de costos de producción; y facilita el avance de las nuevas tecnologías.

La normalización promueve la creación de un idioma técnico común a todas las organizaciones y es una contribución importante para la libre circulación de los productos industriales. Además, tanto en el mercado local como a nivel global, fomenta la competitividad empresarial, principalmente en el ámbito de las nuevas tecnologías.

2.1.11 Normas

Se conoce como norma a la regla o un conjunto de estas, una ley, una pauta o un principio que se impone, se adopta y se debe seguir para realizar correctamente una acción o también para guiar, dirigir o ajustar la conducta o el comportamiento de los individuos.

La norma en el plano del auditor o la normalización como actividad es un documento público y, por lo tanto, puede ser consultada, referenciada y usada por quienes lo deseen. Su aplicación es voluntaria, pero, en algunos casos, las autoridades pueden dictar reglamentos obligatorios que hacen referencia a las normas. Las normas ayudan a mejorar la calidad, la seguridad y la competitividad industrial.

Relación con su certificación

La Organización Internacional de Normalización (ISO) define certificación como "atestación por tercera parte relativa a productos, procesos, sistemas o personas", entendiéndose por atestación la actividad que se basa en la decisión tomada luego de la revisión y consiste en autorizar y emitir una declaración de que se ha demostrado que se cumplen los requisitos especificados. Esta declaración puede ser un certificado o una marca de conformidad. En todos los casos la declaración garantiza a los usuarios de la evaluación de la conformidad que se cumplen los requisitos especificados (futura ISO/IEC 17000).

Para que la certificación se realice en forma imparcial debe ser realizada por una tercera parte, es decir, un organismo independiente de los respectivos intereses del proveedor del objeto de la certificación (primera parte) y del usuario de la certificación (segunda parte).

En México, la normalización está plasmada en las Normas Oficiales Mexicanas (NOM) de carácter obligatorio, elaboradas por dependencias del Gobierno Federal y las Normas Mexicanas (NMX) de ámbito primordialmente voluntario, promovidas por la Secretaría de Economía y el sector privado, a través de los Organismos Nacionales de Normalización.

2.1.12 Acerca De Las Normas ISO

Las normas ISO son un conjunto de estándares con reconocimiento internacional que fueron creados con el objetivo de ayudar a las empresas a establecer unos niveles de homogeneidad en relación con la gestión, prestación de servicios y desarrollo de productos en la industria.

Las iniciales ISO son el acrónimo de International Organization for Standardization, y sus orígenes se remontan 1946, como unión de otros organismos que existían previamente y cuyo objetivo era la regulación y establecimiento de estándares para la fabricación (International Federation of National Standardizing (ISA) y la United Nations Standards Coordinating Committee (UNSCC)) a la reunión inicial, que tuvo lugar en el Instituto de Ingenieros Civiles de Londres, asistieron 64 delegados en representación de 25 países.

Desde entonces y hasta la fecha se han creado más de 23.000 estándares que cubren multitud de áreas de gestión, tecnologías y procesos de producción. Se trata de una organización no gubernamental, en la que se encuentran presentes en 164 países, con 781 comités y subcomités técnicos implicados en el desarrollo de estándares, y que tienen su secretaria Central en Ginebra, Suiza. No es otro que establecer unos niveles reconocidos de cumplimiento de calidad, eficiencia y seguridad en relación con las áreas y actividades concretas que desarrolla cada norma. En la actualidad existen normas de gestión de calidad, gestión de medio ambiente, gestión de seguridad de la información, gestión del riesgo, etc., que permiten a las empresas y organizaciones certificarse en diferentes áreas de cumplimiento en función de las actividades y negocios que desarrollen.

Una de las ventajas importantes que logran las organizaciones con la implantación de las normas ISO, es aportar un valor diferencial frente a la competencia al tratarse de estándares certificados y reconocidos a nivel internacional, que son revisados y auditados de forma periódica con el fin de garantizar el cumplimiento de estos. Esto mejora la percepción de las

empresas tanto para clientes como para accionistas, inversores o socios que puedan mostrar interés en ellas.

Otras mejoras importantes que se logran al implantar una norma ISO en una organización es la optimización de procesos al disponer de más datos y registros sobre los mismos, facilitando la toma de decisiones por parte de la dirección con información más concreta y verificable en todo momento. Además, se facilita la correcta adecuación a las normativas y requerimientos que se puedan tener de clientes u otras entidades y organizaciones pudiendo evidenciar el cumplimiento de estos de una forma documental y fiable, lo cual redundará en mayores niveles de confianza tanto de forma interna como a terceros.

2.1.13 Ventajas De Las Normas ISO Ante Sociedad Y Mercados

Una de las ventajas importantes que logran las organizaciones con la implantación de las normas ISO, es aportar un valor diferencial frente a la competencia al tratarse de estándares certificados y reconocidos a nivel internacional, que son revisados y auditados de forma periódica con el fin de garantizar el cumplimiento de estos. Esto mejora la percepción de las empresas tanto para clientes como para accionistas, inversores que puedan mostrar interés en ellas.

Otras mejoras importantes que se logran al implantar una norma ISO en una organización es la optimización de procesos al disponer de más datos y registros sobre los mismos, facilitando la toma de decisiones por parte de la dirección con información más concreta y verificable en todo momento. Además, se facilita la correcta adecuación a las normativas y requerimientos que se puedan tener de clientes u otras entidades y organizaciones pudiendo evidenciar el cumplimiento de estos de una forma documental y fiable, lo cual redundará en mayores niveles de confianza tanto de forma interna como a terceros.

2.1.14 ISO 20000

Es la norma internacional más reconocida para los sistemas de gestión de TI. Actualmente se encuentra en su tercera versión (2018). La naturaleza de la norma ISO/IEC 20000 permite aplicarla a toda la gama de sectores, ámbitos y actividades empresariales. Su alcance puede limitarse a áreas definidas de la organización o ampliarse para cubrir todas las actividades

internas y las necesidades de los clientes. Ayuda a las organizaciones a establecer la política y los objetivos de la gestión de servicios y a comprender cómo se pueden gestionar los aspectos importantes, aplicar los controles necesarios y establecer objetivos claros para mejorar la prestación de servicios de TI.

Permite que una organización gestione su obligación de cumplir con los requisitos legales aplicables y otras obligaciones de las partes interesadas, y comprobar periódicamente el estado de cumplimiento. Esto permite una mejora continua del sistema de gestión para aumentar su rendimiento.

La norma ISO 20000 está diseñada para ser compatible y armonizada con otras normas reconocidas de sistemas de gestión, incluida la ISO 9001. Por tanto, es ideal para su integración en los sistemas y procesos de gestión existentes.

2.1.15 TI En México

Las TIC engloban los procesos de gestión y difusión de información a través de tecnologías (informática de las comunicaciones, telemática y de interfaces), y los de la comunicación (radio, televisión, telefonía). Ambas ramas de actividad cada vez están más interconectadas, con la progresiva concentración de la prestación de servicios por las mismas empresas, como por ejemplo las empresas de telefonía que van incluyendo servicios de televisión por Internet en su oferta.

El sector de las Tecnologías de la Información y Comunicación (TIC) en México ha crecido exponencialmente desde mediados de los años 80, aumentando su aportación al PIB hasta alcanzar desde 2006 niveles similares a los de países de la OCDE. En 2020, la participación del sector TIC en el PIB de México fue del 3,4%. A ello contribuyó de forma significativa la reforma constitucional en materia de telecomunicaciones y radiodifusión de 2013, promoviendo la entrada de nuevos actores y el desarrollo tecnológico del país. Desde la reforma, el sector ha experimentado una caída en los precios, aumentos en competencia, calidad en los servicios, oferta e inversión en infraestructuras, y mejoras tecnológicas.

2.2 Marco Conceptual

Los conceptos son herramientas valiosas para aproximarnos cognitivamente a nuestro objeto de investigación. Pero lo son solo en la medida en que sean finos, precisos. De otro

modo se convierten en fuentes de ambigüedad y confusión. A continuación, se presentan términos para obtener una mejor comprensión de lo que se va a realizar.

2.2.1 Ingeniería en Sistemas Computacionales

Def. La ingeniería de sistemas es un campo interdisciplinario de la ingeniería que permite estudiar y comprender la realidad, con el propósito de implementar u optimizar sistemas complejos. Puede también verse como la aplicación tecnológica de la teoría de sistemas a los esfuerzos de la ingeniería, adoptando en todo este trabajo el paradigma sistémico. La ingeniería de sistemas integra otras disciplinas y grupos de especialidad en un esfuerzo de equipo, formando un proceso de desarrollo centrado.

2.2.2 Informática

Def. La informática, también llamada computación, es el área de la ciencia que se encarga de estudiar la administración de métodos, técnicas y procesos con el fin de almacenar, procesar y transmitir información y datos en formato digital. La informática abarca desde disciplinas teóricas (como algoritmos, teoría de la computación y teoría de la información) hasta disciplinas prácticas (incluido el diseño y la implementación de hardware y software).

2.2.3 Digitalización

Def. La digitalización es un proceso mediante el cual, algo real (físico, tangible) es pasado a datos digitales para que pueda ser manejado por una computadora (de naturaleza, a su vez, digital), modelándolo, modificándolo, y aprovechándolo para otros propósitos distintos de su cometido o función originales.

2.2.4 Digitalización de Procesos

Def. La digitalización de procesos en la mayoría de los casos en los negocios se refiere a mejorar los procesos, las funciones y operaciones comerciales mediante el aprovechamiento de la nueva tecnología que proporciona el espacio digital.

2.2.5 Tecnologías De La Información (TI)

Def. El concepto de tecnología de la información refiere al uso de equipos de telecomunicaciones y computadoras (ordenadores) para la transmisión, el procesamiento y el almacenamiento de datos. La noción abarca cuestiones propias de la informática, la electrónica y las telecomunicaciones.

2.2.6 La Auditoria

Def. La actividad de auditar o la auditoria es una actividad que consiste en realizar un examen de los procesos y de la actividad económica de una organización para confirmar si se ajustan a lo fijado por las leyes o los buenos criterios. La persona encargada de realizar dicha evaluación recibe el nombre de auditor. Su trabajo implica analizar detenidamente las acciones de la empresa y los documentos donde las mismas han sido registradas y determinar si las medidas que se han tomado en los diferentes casos son adecuadas y han beneficiado a la compañía.

2.2.7 La Auditoría Informática

Def. La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. De esta forma la auditoría informática sustenta y confirma la consecución de los objetivos tradicionales de auditoría.

2.2.8 Normas

Def. Se conoce como norma a la regla o un conjunto de estas, una ley, una pauta o un principio que se impone, se adopta y se debe seguir para realizar correctamente una acción o también para guiar, dirigir o ajustar la conducta o el comportamiento de los individuos.

2.2.9 Normalización

Def. La normalización puede ser comprendida como la actividad que tiene por objeto establecer, ante problemas reales o potenciales, disposiciones destinadas a usos comunes y repetidos, con el fin de obtener un nivel de ordenamiento óptimo en un contexto dado, que puede ser tecnológico, político o económico.

2.2.10 Normas ISO

Def. Las normas ISO son un conjunto de reglamentos y disposiciones de aplicación universal, que se proponen garantizar condiciones mínimas de calidad, tiempos de entrega y niveles de servicio en diferentes tipos de empresas y organizaciones.

2.3 MARCO METODOLÓGICO

En el siguiente apartado se menciona el proceso utilizado para el desarrollo del proyecto. Estas prácticas se apoyan unas a otras y su selección tiene origen mediante toda investigación y planificación.

Estudiar y analizar los pasos necesarios para realizar una auditoria haciendo uso de libros, artículos, auditorías ya documentadas, sitios web, etc. Con el fin de establecer un plan de acción.

Investigar qué puntos establece la norma ISO 20000 haciendo el uso de artículos, documentación, webinar, etc., y basar un plan en base a su implementación para adaptar el proceso de auditoría.

Se realizará un levantamiento de información de forma detallada que permita identificar las necesidades que presentan los servicios en el área de sistemas/TI por la empresa Maikai Tec, con el fin de formular un plan de mejoras que se busca realizar como apoyo a la gestión de aplicaciones, para ello se tomara como base las mayores necesidades, así se podrán plantear soluciones que signifiquen mejoras para los factores que influyen en la correcta operación.

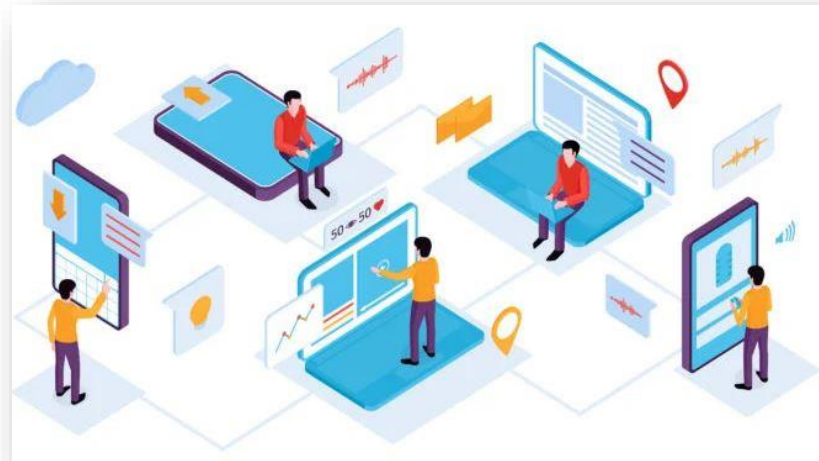
Reconocer el área con la ayuda de los encargados (ingenieros, licenciados, técnicos) del departamento de sistemas/soporte, para definir los procesos que serán auditados, con el fin de poder analizarlos según la norma ISO 2000.

En este diagnóstico, se enfatiza el encontrar un apropiado proceso para plantear oportunidades de mejora en la gestión de servicios, para el sistema de procesos, este sistema funciona de tal manera que los servicios deben estar centralizados, se basa en un aplicativo ejecutado por diferentes clientes, la información es consultada mediante una breve encuesta al cliente, de acuerdo con los permisos concedidos por la empresa Maikai Tec, por tal motivo se deben crear propuestas las cuales permitan que el proceso sea correcto y satisfactorio.

Analizar los procesos/recursos de TI con los que se cuente dentro del departamento de sistemas/soporte, haciendo uso de herramientas de auditoría (entrevistas, encuestas, cuestionarios, etc.) para realizar una medición de su calidad.

Medir la calidad de los procesos auditados con el uso de herramientas basadas en la norma ISO correspondiente para ser integradas de manera documental al expediente de resultados de la auditoría realizada.

Y finalmente presentar los resultados obtenidos mediante la documentación y recursos gráficos a los encargados del departamento de sistemas/soporte para fundamentar el nivel y recomendaciones para el área auditada.



CAPÍTULO III

DESARROLLO Y RESULTADOS.

3.1 Objetivo 1. Reconocer.

Descripción de la Actividad.

Reconocer el área con la ayuda de los encargados (ingenieros, técnicos, licenciados) del departamento de sistemas, para definir los procesos que serán auditados, con el fin de poder analizarlos según la norma ISO 20,000.

3.1.1 Visitar el área de Trabajo.

Procedimiento de trabajo de Maikai Tec.

Contactar clientes

Ejecutivos ya cuentan con cartera de clientes, pero de igual forma su función es la prospección de nuevos clientes. En el caso de seguimiento de cartera se ponen en contacto con ellos para presentarse junto con la empresa en productos y/o servicios que se ofrecen y en el caso de prospección se inicia investigando a la empresa por ejemplo ubicación, contacto en compras y/o soporte enviando carta de presentación.

Una vez realizada la presentación se procede con cotizaciones dependiendo los requerimientos de la empresa, ya sea papelería de oficina, insumos, consumibles o equipo de cómputo.

Al confirmar una compra la empresa automáticamente se vuelve cliente de Maikai Tec por lo que puede mandar el comprobante de pago junto con la Orden de compra.

Pedidos

Maikai Tec cuenta con diferentes mayoristas de acuerdo con la categoría de producto, por lo que es más sencillo encontrar los productos requeridos por el cliente por medio de las páginas web de cada mayorista. Después de encontrar el producto se realiza la cotización y se manda al cliente. Una vez aceptada la cotización se procede con la compra del producto para que llegue a las instalaciones de Maikai Tec.

Recepción

Una vez que llega la mercancía se revisa y que confirma que el producto no venga dañado y/o abierto dado sea el caso se regresa el producto y se pide nuevamente. Después se da de alta en el sistema (Algunos productos tienen número de serie para identificarlos) y se avisa que ya está dado de alta para que el vendedor pueda realizar la factura.

Facturación

El vendedor debe confirmar que el producto ya está en almacén para que posteriormente se realice la factura. La factura se realiza mediante un sistema ERP llamado Aspel.

Entrega

El vendedor coordina la entrega junto con el área de logística para que se pueda entregar al cliente. Una vez entregado el cliente deberá poner en escrito de la factura del lado de pagaré su nombre, fecha y firma del producto entregado en su totalidad. Algunos clientes manejan un portal especial para subir facturas, una vez entregado el producto se puede subir la factura a dicho portal para que realicen el pago.

De acuerdo con los procesos que se tiene en la empresa Maikai Tec, el de ventas se cataloga como uno de los principales y más importantes dentro de la empresa. Se cuenta con personal capacitado para llevar a cabo cada una de las acciones realizadas.

El departamento de TI es de vital importancia en cada una de las organizaciones y/o empresas, grandes o pequeñas, ya que son las encargadas de mantener a flote el área de sistemas.



PROCEDIMIENTO DE LEVANTAMIENTOS

Clientes

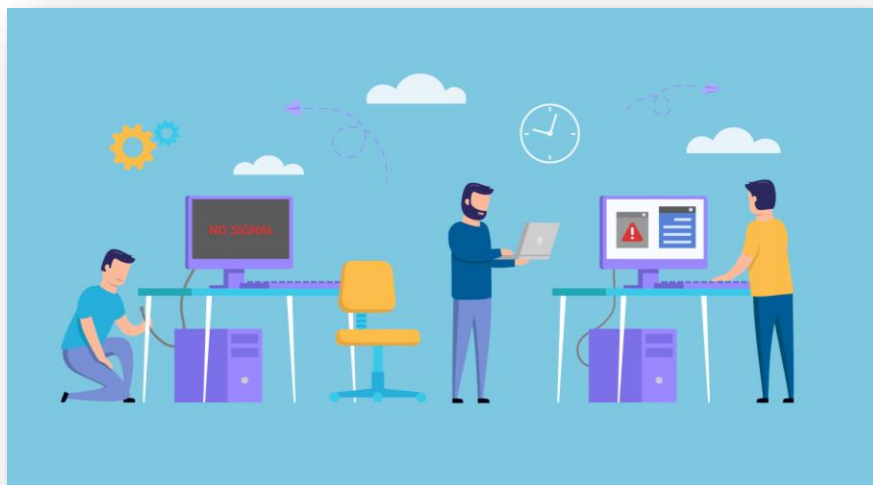
Los clientes, empresas o marcas se contactan directamente con las vendedoras o la directora general, de manera que se hace una previa vista de lo solicitante, mediante un escrito con evidencias mostrando lo que se requiere.

Cotización

El personal capacitado del departamento de sistemas dentro de Maikai Tec, acude al área solicitada, analiza y comprueba la situación, regresando a las instalaciones de la empresa (Maikai Tec) se realiza una cotización previa a los gatos que se van a adquirir, para poder llevar a cabo la reparación.

Levantamiento

Si el cliente aprueba la cotización, se propone una fecha prevista para acudir y realizar el trabajo. Una vez echo todo eso, se toman evidencias de el antes y el después de dicho levantamiento, adjuntándoselas al cliente.



PROCEDIMIENTO DE SOPORTE TECNICO

Clientes

Los clientes, empresas o marcas se contactan directamente con las vendedoras o la directora general, de manera que se hace una previa vista de lo solicitante, mediante un escrito con evidencias mostrando lo que se requiere, por lo regular siendo artículos de TI.

Revisión y cotización

El personal capacitado del departamento de sistemas dentro de Maikai Tec, hace una evaluación y una cotización de lo solicitado por el cliente. Una vez que el cliente accede o no a la cotización, ya sea que el cliente mismo envíe el artículo por su cuenta o el repartidor (trabajador de Maikai Tec) acude a la dirección otorgada por el cliente, trayendo el o los artículos a las instalaciones de la empresa.

Entrega

Ya el o los artículos se encuentren en las instalaciones de Maikai Tec, el personal del área de sistemas se encarga de realizar el soporte técnico, tomando evidencias del antes y un después, llevando un registro de todo lo elaborado, para después adjuntárselas al cliente.

Se termina el proceso de soporte técnico y el repartidor se encarga de llevar lo perteneciente al cliente.



3.1.2 Actividad 2. Selección de los procesos para auditar / Elaboración de cuestionarios de preauditoria.

Descripción del Objetivo:

Para tener un criterio del medio de trabajo se sigue una metodología de auditoría general, y los criterios del modelo de la ISO 20000 que nos dan un marco de referencia y de trabajo estandarizado, que involucran documentos con temas clasificados a través de dominios, procesos y actividades.

Para identificar las áreas que serán auditadas, se usará un grupo de matrices o encuestas para trabajar con ellas durante todo el proceso de preauditoria y que sirven para hacer el análisis de prioridades que dará información de fuentes directas como la dirección general, departamento de sistemas, y usuarios finales para hacer la priorización y la auditoría.

3.1.3. Actividad 3. Políticas de Confidencialidad / Recolección de Datos

Descripción de la Actividad:

En esta actividad se realiza un apartado legal que tendremos que considerar para el uso y manejo de información confidencial dentro de los formatos de entrevistas, cuestionarios, documentación y cualquier otro archivo que represente una extracción de datos que deban ser analizados, medidos o interpretados exclusivamente por el equipo auditor. Esta medida legal nos protege y nos da un voto de fiabilidad ante la empresa que estaremos auditando.

Puntos para tratar:

- a) Datos de los responsables del dominio.** En ellos se incluye la información personal y de contacto del encargado del uso y mantenimiento de los datos recogidos por el sitio web. Asimismo, la información suministrada por la notificación de ficheros de la Agencia de Protección de Datos en el caso de México.

- b) Forma de contacto.** Información para que cualquier usuario pueda ejercer sus derechos de privacidad, acceso, rectificación, cancelación y oposición, según los Derechos ARCO en México.
- c) Finalidad del uso de datos.** Deben estar contemplados toda la información sobre el objetivo y el tratamiento de los datos, así como sus responsables. A su vez, se debe especificar el porqué del uso de la información y el tiempo.
- d) Cesión o transmisión.** Seguro has escuchado o leído sobre esto últimamente y es que la posibilidad que tienen las aplicaciones y sitios web para compartir datos personales de sus usuarios es un hecho muy delicado. Aquí debe estar muy especificado si tus servicios, web o app comparten los datos de los usuarios con terceros y por qué.
- e) Responsabilidades del usuario.** Así como el usuario tiene derecho, también tiene deberes. En este punto se plantean todas las limitaciones que tienen las personas para usar, transmitir y divulgar los servicios e información de tu empresa, sitio o aplicación.

La confidencialidad debe ser ejercida por el auditor bajo criterios de autonomía, respeto por los demás y confianza, apegándose a leyes y normativas que regulan la profesión, lo cual incidirá directamente en la percepción que pueda tener el entorno sobre el auditor como profesional que atiende el interés público.

3.1.4 Actividad 4. Matriz Diagnóstica – Prioridades y Riesgos

Descripción de la Actividad

En esta actividad se realizará una síntesis de preguntas que se aplicará a los miembros del departamento de sistemas para una preauditoria lo cual nos arroja la información adecuada que será usada para determinar la importancia, funcionalidad y operabilidad de acuerdo con los directivos y usuarios que tienen accesos a los servicios brindados por el departamento de

sistemas. Presenta los objetivos de control relevantes que pueden ser enfocados en la organización, mediante el levantamiento de la información del formulario:

Cuya pregunta principal se centra en el nivel de riesgo que el encuestado identifica en cada una de las actividades. La calificación puede ir desde de 1 hasta 5, siendo 1 el menos importante y 5 el más importante;

El segundo parámetro es el funcionamiento, en el que se identifica cuál es el nivel de funcionamiento actual, que va desde no se hace o se hace muy mal hasta se hace muy bien calificándose con valores desde 1 a 5 respectivamente;

Existe una tercera pregunta que consulta sobre quién lo realiza, para lo cual existen varias alternativas:

- a) Puede ser realizado por el departamento de sistemas, o por otros dentro de la misma empresa.
- b) Por externos como outsourcing o contratados para tareas específicas.
- c) O puede existir la posibilidad de que la persona consultada no esté al tanto de quien es el encargado.

La cuarta y quinta pregunta tratan de identificar si las actividades son controladas y formalizadas:

- a) A través de documentos aprobados por la administración de la empresa, a estos controles se les llama: “Auditado” O “No auditado”.
- b) Y lo que es “Formalizado” O “No formalizado” se refiere si existe algún documento que norme la forma de realizar las actividades consultadas.

La última pregunta es quién es el responsable, es decir cuál es el nombre de la persona encargada de las tareas relacionadas con la actividad consultada.

La información de esta encuesta será tomada como parte principal de la selección de las áreas auditables.

Control de evaluación realizada:				01-02	
Tabla de validación para la ejecución de “Matriz de Diagnostico – Prioridades y Riesgos”.					
Área involucrada	Departamento de Sistemas	No. De Integrantes Involucrados	03	Actividad correspondiente al día de Calendarización:	00 / 00 / 1999

Formulario de Entidad No. 1	
Departamento: <u>Departamento de Sistemas.</u>	Cargo: <u>Jefe de departamento</u>

Importancia	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;">Desempeño</td> <td style="width: 50%; text-align: center;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;">Control Interno</td> <td style="width: 50%; text-align: center;">WP Ref.</td> </tr> </table> </td> </tr> </table>	Desempeño	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;">Control Interno</td> <td style="width: 50%; text-align: center;">WP Ref.</td> </tr> </table>	Control Interno	WP Ref.
Desempeño	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;">Control Interno</td> <td style="width: 50%; text-align: center;">WP Ref.</td> </tr> </table>	Control Interno	WP Ref.		
Control Interno	WP Ref.				

	Muy Importante	Algo Importante	No Importante	No está seguro	No se aplica		Excelente	Muy Bueno	Satisfactorio	Pobre	No está seguro	Dimensionado Formalmente	No Dimensionado	No se aplica	Documentado	No documentado	No está seguro	
Procesos de TI																		
Planificación y organización																		
5						P1 Definir un plan estratégico de TI.			5								1	5
	4					P2 Definir la arquitectura de la información.					3				3			4
5						P3 Determinar la dirección tecnológica.			5							2		4
5						P4 Definir la organización y las relaciones de TI.		6							3			4
	4					P5 Administrar la Inversión de TI.		6							3			5
	4					P6 Comunicar los objetivos y direcciones de la gerencia.		6								2		3
	4					P7 Administrar los recursos humanos.			5						3			2
5						P8 Asegurar el cumplimiento de los requerimientos externos		6							3			4
5						P9 Administrar la calidad.					3						1	2
5						P10 Administrar proyectos.			5							2		4
5						P11 Evaluar los riesgos.		6									1	3
Adquisición e implementación																		
5						A1 Identificar soluciones automatizadas.		6								2		3
5						A2 Adquirir y mantener software de aplicación.	7								3			4
5						A3 Adquirir y mantener infraestructura de tecnología.	7								3			4
5						A4 Desarrollar y mantener procedimientos.			5								1	3
5						A5 Administrar cambios.		6								2		4
5						A6 Instalar y acreditar sistemas.	7								3			5
Entrega y soporte																		
	4					E1 Definir y administrar niveles de servicio.				4							1	3
5						E2 Administrar servicios de terceros.		6								2		5
5						E3 Administrar el rendimiento y la capacidad.			5						3			4
5						E4 Asegurar un servicio continuo.		6								2		3
5						E5 Asegurar seguridad de sistemas.			5						3			5
5						E6 Identificar y asignar costos.	7								3			5
5						E7 Educar y capacitar a los usuarios.			5							2		3
5						E8 Asistir y asesorar a los clientes.			5							2		3
5						E9 Administrar la configuración.			5						3			5
5						E10 Administrar problemas e incidentes.		6								2		4
5						E11 Administrar datos.			5							2		4

Tabla 1 “Matriz de Diagnostico – Prioridades y Riesgos”

3.1.5 Actividad 5. Formulario de Evaluación del Riesgo

Descripción de la Actividad:

Está actividad comprende la evaluación del riesgo de auditoría el cual es el requisito básico para verificar qué y cuándo deben medirse los procesos y productos de calidad para obtener los máximos beneficios para la organización. No obstante, con frecuencia, saber la respuesta a ese “qué” y “cuándo puede” ser un gran desafío.

Es necesario en este sentido tener en cuenta lo siguiente:

- La evaluación de los riesgos inherentes a los diferentes subprocesos de la auditoría.
- La evaluación de las amenazas o causas de los riesgos.
- Los controles utilizados para minimizar las amenazas o riesgos.
- La evaluación de los elementos del análisis de riesgos.

Generalmente se habla de riesgo y conceptos de riesgo en la evolución de los sistemas de control interno, en los cuales se asumen tres tipos de riesgo:

- **Riesgo de Control:** Que es aquel que existe y que se propicia por falta de control de las actividades de la empresa y puede generar deficiencias del sistema de control interno.
- **Riesgo de Detección:** Es aquel que se asume por parte de los auditores que en su revisión no detecten deficiencias en el sistema de control interno.
- **Riesgo Inherente:** Son aquellos que se presentan inherentes a las características del sistema de control interno.

Sin embargo, los riesgos están presentes en cualquier sistema o proceso que se ejecute, ya sea en procesos de producción como de servicios, en operaciones financieras y de mercado, por tal razón podemos afirmar que la auditoría no está exenta de este concepto.

Para llenar este formulario se ha tenido en cuenta las respuestas emitidas por los encuestados y de ahí se ha realizado un resumen que ayuda a calificar las actividades de acuerdo con el orden de importancia y de riesgo. En la sección titulada “importancia” se puede tener resultados como:

- a) Muy importante.
- b) Algo importante.
- c) No importante.
- d) No se aplica.

Para medir el riesgo, se han planteado las siguientes posibilidades:

- a) Alto.
- b) Medio.

- c) Bajo.
- d) Inmaterial.
- e) No está seguro.

Control de evaluación realizada:				02-02	
Tabla de validación para la ejecución de <i>“Matriz de Diagnostico – Prioridades y Riesgos”</i> .					
Área involucrada	Departamento de Sistemas	No. De Integrantes Involucrados	03	Actividad correspondiente al día de Calendarización:	00 / 00 / 1999

Formulario de Entidad No. 3			
Departamento:	Departamento de Sistemas	Cargo:	Soporte y atención de TI

Importancia						Desempeño										Control Interno		WP Ref.
Muy Importante	Algo Importante	No Importante	No está seguro	No se aplica		Excelente	Muy Bueno	Satisfactorio	Pobre	No está seguro	Dimensionado Formalmente	No Dimensionado	No se aplica	Documentado	No documentado	No está seguro		
Procesos de TI																		
Planificación y organización																		
5					P1 Definir un plan estratégico de TI.			4						2		5		
	4				P2 Definir la arquitectura de la información.					2				2		4		
5					P3 Determinar la dirección tecnológica.					2				2		4		
5					P4 Definir la organización y las relaciones de TI.			5						2		4		
	4				P5 Administrar la Inversión de TI.		6							3		5		
	4				P6 Comunicar los objetivos y direcciones de la gerencia.			5						2		3		
	4				P7 Administrar los recursos humanos.			5						3		2		
5					P8 Asegurar el cumplimiento de los requerimientos externos			5						3		4		
5					P9 Administrar la calidad.			5							1	2		
5					P10 Administrar proyectos.			5						2		4		
5					P11 Evaluar los riesgos.			5							1	3		
Adquisición e implementación																		
5					A1 Identificar soluciones automatizadas.			4						2		3		
5					A2 Adquirir y mantener software de aplicación.	7								3		4		
5					A3 Adquirir y mantener infraestructura de tecnología.	7								3		4		
5					A4 Desarrollar y mantener procedimientos.					2					1	3		
5					A5 Administrar cambios.			5						2		4		
5					A6 Instalar y acreditar sistemas.	7								3		5		
Entrega y soporte																		
	4				E1 Definir y administrar niveles de servicio.				3					2		3		
5					E2 Administrar servicios de terceros.		6							2		5		
5					E3 Administrar el rendimiento y la capacidad.			5						3		4		
5					E4 Asegurar un servicio continuo.		6							2		3		

5					E5 Asegurar seguridad de sistemas.		6						3			5
5					E6 Identificar y asignar costos.	7							3			5
5					E7 Educar y capacitar a los usuarios.		6							2		3
5					E8 Asistir y asesorar a los clientes.			5						2		3
5					E9 Administrar la configuración.			5					3			5
5					E10 Administrar problemas e incidentes.		6							2		4
5					E11 Administrar datos.			5						2		4

Tabla 2 “Matriz de Diagnostico – Prioridades y Riesgos”

3.2 Objetivo 2. Planeación de la auditoria / Herramientas para la ejecución y plan de trabajo.

Descripción del Objetivo.

En esta etapa de desarrollo se tomarán en cuenta todas las herramientas para planificar nuestra auditoria y tener las herramientas necesarias para documentar cada estancia de está. Con esta información se pueden establecer los objetivos necesarios para planificar el proceso de la auditoría y su tiempo de ejecución (conocer los recursos técnicos y humanos necesarios para realizarla).

Investigar qué puntos establece la norma ISO 20000 haciendo el uso de artículos, documentación, webinar etc. y basar un plan de acción en base a su implementación para adaptar el proceso de auditoría.

Así mismo analizar los procesos y/o recursos de TI con los que se cuente dentro del departamento de sistemas haciendo uso de herramientas de auditoría (entrevistas, encuestas, cuestionarios etc) para realizar una medición de su calidad.

- **Aplicar**
- **Medir:** La calidad de los procesos auditados con el uso de herramientas basadas en la norma ISO correspondiente para ser integradas de manera documental al expediente de resultados de la auditoría realizada.

3.2.1 Actividad 1. Formular proceso de auditoría.

Descripción del Objetivo

En esta actividad se pondrán en práctica aquellas herramientas que constatan el plan de auditoría, así como tener ya en cuenta los niveles de riesgo para poder tener un accionar acorde a nuestro fundamento.

La auditoría en informática siendo un proceso básico de validación y control del uso de los recursos tecnológicos utilizados en el logro de las estrategias, debe también contemplar como parte de sus actividades primarias el entendimiento del entorno que rodea al negocio, así como de la estructura y tiempos del plan estratégico de negocios.

La función de auditoría informática debe contar también con un desarrollo de actividades basadas en un método de trabajo formal, que sea entendido por todos los auditores de informática y complementado con técnicas y herramientas propias de la función.

3.2.2 Actividad 2. Reconocer bases de la norma ISO 20000.

ITIL e ISO 20000

La gestión de los servicios TIC es un aspecto clave para un proveedor de servicios, por lo que buscar la alineación con las metodologías y normas de referencia en el sector representa un aspecto muy importante para la mejora de los procesos de negocio. En este sentido el conjunto de mejores prácticas descritas en la biblioteca ITIL (Infrastructure Technology Information Library), que fue creada por el Gobierno Británico en la década de los 80 y que ha ido evolucionando con la participación de distintos foros y grupos de interés del sector TIC hasta convertirse en un modelo de referencia ampliamente aceptado, sirve como referencia para la gestión de servicios TI.

ITIL proporciona una descripción detallada de una serie de buenas prácticas de TI, a través de una amplia serie de roles, tareas, procesos y responsabilidades que pueden adaptarse a cualquier organización de TI.

ITIL ofrece un marco común para todas las actividades del área TI, como parte de la provisión de servicios. Estas actividades se dividen en procesos, que usados en conjunto proporcionan un marco eficaz para lograr una gestión de servicios TI más madura. Cada uno de estos procesos cubre una o más tareas del área TI como desarrollo de servicio, gestión de infraestructuras y provisión y soporte de los servicios. Este planteamiento del proceso

permite, por tanto, describir las mejores prácticas de la gestión de servicios TI independientemente de la estructura adoptada por la organización.

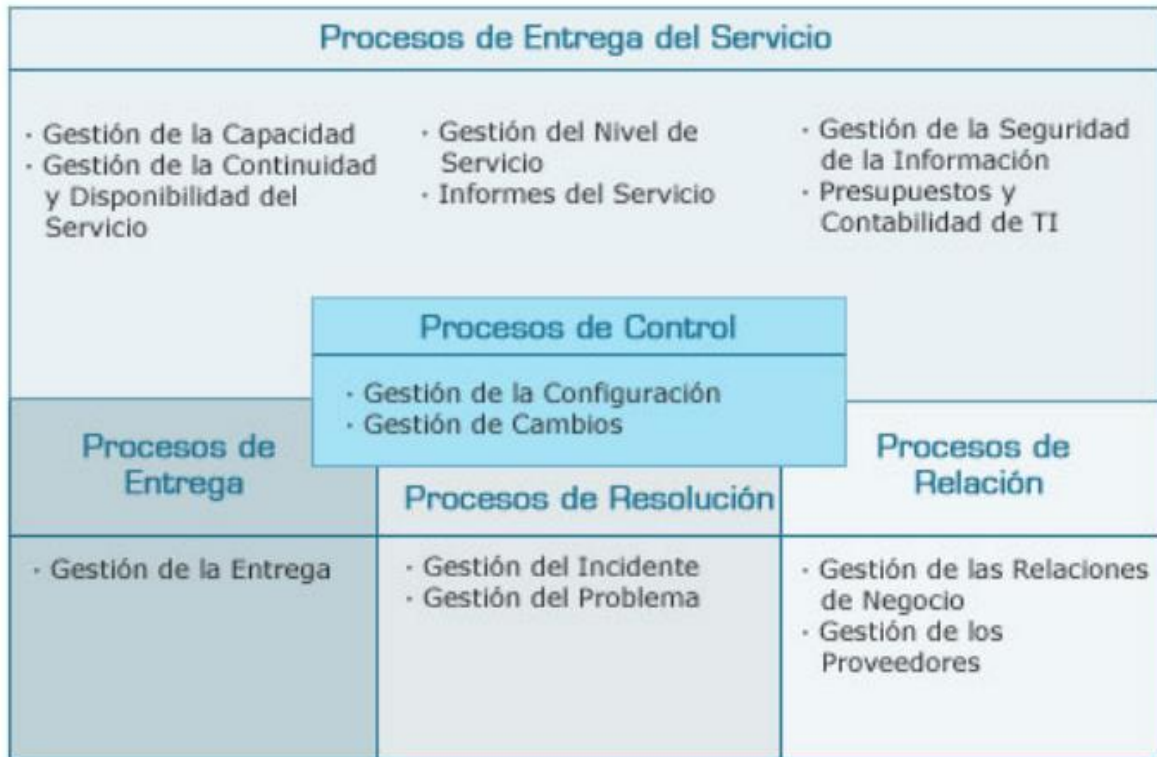


Figura 1. Proceso ISO 20000

Esta norma se compone de dos partes:

1. ISO/IEC 20000-1:2005 Tecnología de la Información – Gestión de Servicios- Parte 1:

Especificaciones, que determina los requisitos del sistema de gestión de servicios TI de una organización y puede utilizarse para su aplicación interna por las organizaciones para certificación o con fines contractuales.

2. ISO/IEC 20000-2:2005 Tecnología de la Información – Gestión de Servicios- Parte 2:

Código de Buenas Prácticas, que proporciona recomendaciones sobre las mejores

prácticas para la gestión de los servicios de TI y se recomienda como guía para aquellas organizaciones cuya alta dirección desee ir más allá de los requisitos de la norma. La estructura de la norma responde a la de un sistema de gestión de servicios TI basado en procesos que pueden gestionarse mediante el ciclo PDCA o de mejora continua. Un enfoque que favorece la integración con otros sistemas de gestión, y muy especialmente con las normas ISO 9000 con las que además comparte principios.

Un conjunto de valores orientados a fomentar determinadas pautas de comportamiento en las personas de la organización para conseguir un mejor desempeño: el enfoque a procesos, la mejora continua o la participación de los trabajadores, etc. cuya implantación como veremos a continuación requiere nuevas formas de trabajar y organizarse en la empresa.

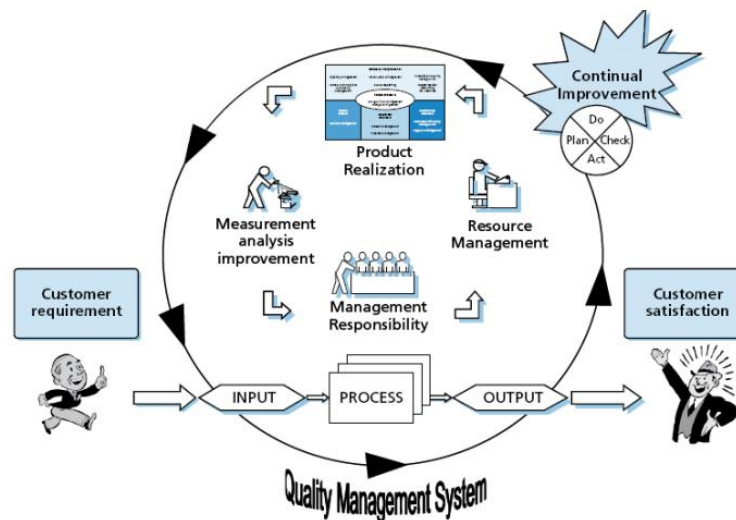


Figura 2. Metodología para la mejora de procesos TI.

La complejidad de las actividades a llevar a cabo y la necesidad de integración de las buenas prácticas de ITIL y los procesos requeridos por el estándar ISO 20000 con los sistemas de gestión ya existente en Alambra Eidos, llevan a la organización a adoptar un modelo secuencial o escalonada, estableciendo diferentes fases en cada una de las cuales la empresa aborda la implantación de los distintos procesos de gestión del estándar.



Figura 3: Metodología para la implantación de los procesos de la norma ISO 20000

La implantación del sistema de gestión de los servicios como un proyecto de mejora es una decisión estratégica, la apuesta de la dirección por la mejora de la calidad está ligada a las personas y en torno a la participación del personal de la organización se mueve la metodología que establece acciones en diferentes ámbitos:

- Documentación

La implantación del sistema exige lanzar acciones de mejora orientadas a la revisión y elaboración de documentación. Se trata de identificar toda aquella documentación común entre los distintos sistemas de gestión para unificarla y conformar un sistema de gestión documental único, que sea ágil y eficiente, que minimice los aspectos burocráticos y que favorezca la integración real entre éstos.

En este sentido la documentación común debe ser referenciada y sólo deben coexistir documentos genéricos o marcos de gestión, en la línea del manual de calidad para los sistemas de gestión de calidad, que sirvan para articular todo el sistema de gestión documental integrado.

- Roles

La definición de nuevos roles dentro de la organización, o la asunción de nuevas responsabilidades en los ya existentes, no solo favorece la implicación desde las primeras etapas de un mayor número de miembros de la organización en el proyecto de implantación sino sirve además como mecanismo de difusión interna.

El hecho de lanzar acciones de mejora relacionadas con la definición de roles hace que la idea del sistema de gestión empresarial único y fiel reflejo de la organización llegue a los distintos niveles de la organización traspasando el equipo de proyecto.

- Diseño de procesos

La implantación de un sistema de gestión integrador exige la revisión y rediseño de procesos. El objetivo es analizar los procesos existentes para detectar en qué medida se deben mejorar para satisfacer los requisitos de otros modelos de gestión, y rediseñar los

procesos para que reflejen no solo los requisitos de las normas sino la realidad de la organización. Evitando así la coexistencia de sistemas de gestión paralelos, con procesos independientes cuyo alcance está limitado a determinados ámbitos de la organización, perdiendo la perspectiva, objetivos, visión y misión real de la organización.

En el diseño de procesos deben participar miembros de la organización de distintos niveles, síntoma este de que el resultado reflejará la manera de trabajar real de la organización, y el sistema de gestión resultante será asumido como propio de manera natural y no se percibirá como un elemento añadido a la organización.

- Indicadores

La eficacia de las mejoras introducidas en la organización debe ser evaluada en base a una serie de métricas bien definidas que contribuyan a la mejora continua. La inclusión de estos indicadores ha de ser también progresiva para que la organización vaya ajustando y asumiendo las mejoras de una manera racional.

- Actividades relacionadas con la formación y comunicación

La visibilidad del proyecto y las mejoras introducidas se potencian mediante acciones orientadas a facilitar que los distintos miembros de la organización participen y se sientan parte del proyecto. Su contribución para lograr los objetivos de la organización se ve favorecido por una mayor capacidad para intervenir, lo que se potencia mediante programas de formación. Estas acciones permiten a su vez consolidar una cultura organizativa orientada a la mejora continua y a la consecución de los objetivos empresariales.



Figura 4: Acciones para la mejora de procesos

3.2.3 Actividad 3. Elaboración de solicitud de auditoria

Descripción de la Actividad

Dentro de esta tarea se debe realizar un oficio o documento que exprese la intención del auditor dentro del departamento a inspeccionar. Es en este momento que se hace del conocimiento al encargado acerca de la norma y los criterios que dicta, así como difundir la información correcta para persuadir de dudas o inquietudes que se pudieran presentarse al realizar nuestra auditoria. Esto debe realizarse en una cita con los responsables del área para poder difundir a la mayor gente involucrada acerca del plan de auditoría y tener un desempeño pleno en el departamento o áreas correspondientes.

Los puntos más importantes para considerar durante la plática y a abordar en la solicitud serán:

- ¿Qué busca evaluar la auditoria?
- ¿Qué departamento(s) se verá(n) involucrado(s)?
- ¿Que alcance y limitaciones tiene nuestra auditoria?
- Integrantes que realizan la auditoría

- e) Establecer los tiempos que tomará realizar dicha evaluación
- f) Conformidad del o los responsables del área

3.2.4. Actividad 4. Elaboración de cuestionarios y rubros apegados al modelo de ISO 20000

Descripción de la Actividad:

El cuestionario tiene como finalidad la recopilación de datos mediante preguntas impresas en cédulas o fichas, en las que el encuestado responde de acuerdo con su criterio; de esta manera, obtendremos información útil que se puede concentrar, clasificar e interpretar por medio de su tabulación y análisis, ya sea para realizar un estudio preliminar de la situación que se está investigando o para sondear el problema en cuestión.

Los cuestionarios serán enfocados para indagar información en dónde tengamos como actores.

A continuación, se presenta una lista de los rubros que comprenderán aquellos cuestionarios con indicadores de riesgo:

3.2.5. Actividad 5. Elaboración de entrevistas y rubros apegados al modelo ISO 20000

Descripción de la Actividad:

La entrevista es una herramienta que será dirigida al personal que está como encargado del área de sistemas dentro del plantel. La entrevista será usada como la principal técnica de recopilación de información teniendo la característica de ser realizada en forma directa, cara a cara y a través de algún medio de captura de datos, el auditor interroga, investiga y confirma directamente con el entrevistado sobre los aspectos que está auditando.

Entender y seguir un procedimiento bien estructurado, servirá al auditor de sistemas para llevar a cabo una buena investigación, apoyado en una serie de preguntas previamente establecidas y enfocadas al objetivo de la entrevista; con este método se busca captar una mayor información sobre lo que se auditará.

ENTREVISTA ACERCA DE LOS PROCESOS Y SERVICIOS DE TI			
Datos de Control			
Fecha de Aplicación:	12/00/1111	Lugar de Aplicación:	Mai Kai Tec. S.A de C.V.
Área auditada:	Departamento de Sistemas		
Datos del Entrevistado			
Funcionario:	Jefe de Sistemas	Años de experiencia dentro de la institución:	1 año con 7 meses
Edad:	25		

Fase 1. Acerca del Empleado.		
No.	Preguntas	Respuesta
1	¿Cuáles son sus obligaciones y responsabilidades como jefe?	Mantener el área de sistemas siempre a la vanguardia, funcional y efectiva.
2	¿Con quién o con qué posiciones se comunica regularmente?	Jefe directo (director general), coordinadores y directores académicos.
3	¿Qué factores tienden a facilitar la efectividad de su trabajo?	La comunicación clara entre el usuario y la correcta especificación del suceso.
4	¿Qué inhibe su efectividad?	La falta de comunicación.
5	¿Qué decisiones toma Ud. normalmente?	Aprobar y realizar procedimientos dentro del área.
6	¿Qué información necesita para tomar estas decisiones?	Estructura, problemática, posibles soluciones y valoración de la problemática, además de una clara comunicación.
7	¿Son políticas formales o informales las que determinan cómo consigue la información?	Son políticas formales, porque se tiene un manual de procedimientos internos.
8	¿Está de acuerdo con estas políticas?	Totalmente, además que siempre se actualizan.
Fase 2. De la Organización y relación con la Operabilidad.		
No.	Preguntas	Respuesta
1	¿Cómo sabe la organización cuándo se ha hecho un buen o mal trabajo?	Todo procedimiento interno realizado se hace notar, además, la buena comunicación dentro del área permite analizar y recaudar información para determinar la efectividad del trabajo.
2	¿Cuáles son sus objetivos personales?	Mantener el área siempre funcional y efectiva a largo plazo.
3	¿Cuáles son las mayores fuerzas o potencias comunicacionales de la organización? Sea específico.	La confianza que hay entre el personal es grata, todo lo que sucede dentro y fuera del departamento siempre se comenta en equipo y se logra una buena comunicación por ende todo siempre tiene pronta solución.
4	¿Cuáles son las mayores debilidades en comunicación que tiene su organización?	Es difícil que haya poca comunicación siempre se procura cuidar ese aspecto dentro de la organización.
5	¿Cuál es para Ud. el mayor problema sin resolver que tiene la organización?	La desconfianza que tienen con el área puesto que la edad que tiene el personal carece de credibilidad al ser muy jóvenes.
6	¿Qué le gustaría ver que se haga acá para mejorar la comunicación?	Una mejora que se podría hacer es programar juntas más seguido para platicar situaciones y crear mejores soluciones además de eficaces.
7	¿Cómo evaluaría la comunicación de parte del departamento?	La comunicación es siempre sincera e instantánea solo que a veces el personal se incomunica por algunos periodos por cuestiones de zonas de alcance de señal interna o externa.

8	¿Se maneja una gestión de calidad en los activos?	Se procura en su mayoría seguir normas de calidad, aunque falta mejorar esa parte, esto por falta de investigación para la perfección de la organización.
9	¿El/los métodos/s que tiene el personal para un control de acceso están bien definidos?	‘No comprendió el tema’.
10	¿El departamento cuenta con normas o reglamentos que aseguren la gestión de la información?	Sí en su mayoría como se mencionó existe un reglamento interno y un manual de procedimientos que redacta todo como se tiene que llevar a cabo dentro de la organización.
Fase 3. De los Recurso de TI existentes y su Capacitación.		
No.	Preguntas	Respuestas.
1	¿Cómo evaluaría a su gente en términos de: • apertura hacia nuevas ideas • deseos de compartir información • habilidad para aclarar expectativas habilidad para coordinar el trabajo en la unidad?	El personal siempre es transparente ante todo incluyendo políticas, procedimientos y comunicación. Se tiene confianza siempre y antes de actuar se platica la situación para procurar cometer errores mínimos siempre están dispuestos a aprender, innovar y mejorar tanto su persona como el área en general.
2	¿Está usted de acuerdo con las reglas para la adquisición, desarrollo y mantenimiento de sistemas de información?	Efectivamente ya que como se mencionó anteriormente existe un manual de procedimientos interno que permite el pleno desarrollo de las múltiples tareas que se llevan a cabo dentro del área.
3	¿Considera que la gestión de los incidentes de la seguridad de la información, están claramente definidos?	Todo lo que sucede y cómo se lleva a cabo este documentado para posteriores incidencias similares esto para mejorar siempre y encontrar debilidades en la seguridad de la información.
4	¿Se brinda monitoreo constante al estado de los equipos de la unidad de tecnología y de todos los departamentos de la institución? (evidencias)	Si gran parte de los equipos tienen monitoreo todo el tiempo ya sea por medio de alarmas y monitoreo físico dictado en la bitácora de monitoreo de equipo especial. La otra parte se divide en revisiones periódicas que son desde horas, días y semanales.
5	¿Se revisa de manera organizada la configuración de los equipos?	Si, para que siempre se tenga un orden de todo lo que se tiene y cómo funciona en el momento además de obtener su máximo rendimiento y funcionamiento efectivo.
6	¿Está de acuerdo con las adquisiciones de licencias de software adquiridas por la institución?	Completamente de acuerdo, todas las licencias que se tienen son las necesarias, además que se tiene un control exhaustivo para la renovación periódica de las licencias, esta parte es de las más importantes ya que se cuenta con una cantidad de equipo bastante importante y lo que menos quiere la institución es tener problemas de licencias con las empresas proveedoras de servicios.
7	¿Se maneja expediente de los equipos que cumplieron con su vida útil?	Así como todo el equipo se tiene inventariado, de igual manera el equipo que está por darse de baja está inventariado y al estar por completo fuera de operación incluso desechado se tiene documentado.
8	¿Las recepciones de solicitud de soporte son enviadas al departamento, de manera formal, ya sea a través de memorando o correo electrónico?	Si, se procura en su totalidad los reportes sean siempre de manera formal para tener un registro de todo lo que se hace dentro del área, esto por correo electrónico así mismo permite que sea atendido a la brevedad.
9	¿El departamento cuenta con el número de funcionarios necesarios para brindar	Al ser una institución comprometida donde se procura siempre tener el equipo funcionando de manera efectiva el

	mantenimiento correctivo a los equipos que presentan fallos y problemas?	personal con el que se cuenta es suficiente para resolver todos los problemas que susciten durante la jornada.
10	¿Se maneja un tipo de acta entrega recepción del equipo?	Si siempre se cuida esa parte, intentar que todo equipo siempre tenga un registro, así como recibos contra entrega para evitar cualquier conflicto a la hora de revisar o entregar, ya que permite una mejor organización en tiempos de reparación, revisión, mantenimiento y solicitudes de equipos para préstamo o asignación a colaboradores.
11	¿Se elabora bitácora del mantenimiento correctivo?	Sí, y en el total de las solicitudes se exigen correos electrónicos para tener una bitácora y documentación de las incidencias.
12	¿Existe alguna normativa o reglamento para la baja de equipos de cómputo?	Sí, existe un manual interno que redacta el procedimiento de toda acción que se lleva internamente específicamente un apartado para la baja de equipo que ha concluido su vida útil, así como la detección de una falla irreparable causante de baja.
13	¿Se establece formato para el reporte para la baja del/los equipo/s de cómputo?	Todo equipo que esté para baja es revisado y se redacta un documento que especifica por que el equipo está en condición de baja con fecha y personal que lo determinó.
14	¿Se tiene estructurado diagrama de flujo para la baja de equipos de cómputo?	Como tal un diagrama de flujo no solo un manual de procedimiento por pasos para su efectiva baja.

Fase 4. De los Servicios y Mantenimientos brindados.

No.	Preguntas	Respuesta
1	¿Se maneja cronograma para la planificación de mantenimiento preventivo?	Sí por que se espera que sea los más rápido y eficaz posible ya que el tiempo de ejecución es limitado, además de que para poder hacerlo en algunos equipos se requiere permiso con anticipación y un horario para evitar interferencia en el trabajo de los colaboradores.
2	En caso de ser Si la respuesta anterior, indique, ¿si se sociabiliza el cronograma con cada una de las dependencias consideradas?	Así es para evitar interferir en el tiempo de los colaboradores de esta manera se tiene un orden y permite ser eficaz en la ejecución.
3	¿Considera usted que la ejecución de los procesos de mantenimiento preventivo es eficiente?	Sí porque detrás de la ejecución se tiene una planeación, un procedimiento y una bitácora de mantenimiento que permite determinar áreas y prioridad.
4	¿Le parecen adecuadas las herramientas, dispositivos, empleadas para realizar mantenimiento a los equipos?	Todo el equipo que se tiene en el departamento es el necesario para atender cualquier situación que se presente y de ser necesario algo que no se tenga a la mano se hace la requisición al departamento de compras con un documento redactando el que y porque se requiere para ser adquirido.
5	¿Se maneja bitácora para el control del mantenimiento preventivo de los equipos?	Si se tiene un esquema que permite identificar todo el equipo que se encuentra dentro de la organización, así como relaciones de inventarios que especifican que y dónde se encuentra todo y una bitácora para saber a qué equipo ya se le dio mantenimiento.
6	¿El tiempo asignado para dar mantenimiento a un equipo, considera usted que es corto?	La mayor parte del equipo si es fácil otra parte por la ubicación donde se encuentra tiene un grado de complejidad más alto y por ende conlleva más tiempo de mantenimiento.
7	¿En los dos últimos años, se tiene el registro de los equipos que han recibido mantenimiento preventivo?	Si el equipo este marcado y se tiene un registro de todo lo que se le ha hecho y cuando, además cada 6 meses de procura hacer mantenimiento preventivo.

8	¿En los dos últimos años, se tiene el registro ordenado por fecha, de las solicitudes para mantenimiento preventivo de los equipos?	Sí, como se mencionó anteriormente existe una bitácora de todo lo que se les hace a los equipos y mantener un orden. Además de un registro estricto de todo lo que se solicita.
9	¿Se tiene estructurado diagrama de flujo para los procesos de mantenimiento?	Sí también se tiene un manual de procedimientos que especifica los procesos ordenados.
Fase 5. Cierre y retroalimentación de la Entrevista.		
No.	Preguntas	Respuesta
1	¿Cómo evaluaría usted la manera en la que el auditor abordó la entrevista?	Atenta y cómoda, todo el tiempo me sentí en confianza y abordé los temas de manera profesional y certera.
2	¿La información recabada piensa que será de utilidad para el departamento?	Si además que ayudó a identificar puntos débiles dentro del departamento, dando puntos de vista para mejorar la eficiencia de este.
3	¿Se sintió cómodo?	Por completo, el auditor es amable, atento y sabe perfectamente los temas que aborda además de hacer preguntas certeras.
4	¿Alguna observación que desee agregar?	Sin observaciones.

Tabla 3. Entrevista acerca de los procesos y servicios TI.

3.2.6 Actividad 6. Cuestionarios de procesos COBIT.

Descripción de la Actividad:

Esté cuestionario contiene los procesos que se abordaron en la selección de auditoría así mismo, tuvimos que definir cada uno de los procesos y aquí se preguntarán si estamos hablando de un proceso por el cual ya preguntamos, pero no, ya que los procesos tienen un dominio, esta área de dominio es la que deben trabajar los integrantes del departamento de sistemas, aquí se cuestionaran a los integrantes si cumplen con el funcionamiento de cada dominio, para posteriormente ser evaluados y medir su nivel de definición de los procesos.

3.2.7. Evaluación de los resultados de los cuestionarios.

Para poder evaluar los procesos COBIT realizaremos el cuestionario en el siguiente orden:

- “Matriz de Evaluación de Dominio de Procesos COBIT – Sección de Definición”
- “Matriz de Evaluación de Dominio de Procesos COBIT”

Con el documento del inciso “a” tendremos los siguientes rubros para calificar cada definición del dominio de los procesos:

- No cumple.
- Cumple levemente.

- Cumple parcialmente.
- Cumple mayoritariamente.
- Cumple casi totalmente.
- Cumple totalmente.

De manera que:

P2	Arquitectura de la información.							66.6666%
	Los objetivos de TI dan soporte al plan estratégico de la institución.					X		83.3333%
	Los proyectos de TI en el portafolio de proyectos se pueden rastrear hacia el plan táctico de TI.			X				50.00%
	Las actualizaciones del plan estratégico de TI se reflejan en actualizaciones de los planes tácticos de TI.				X			66.6666%

El proceso número 2 de la “Planificación y Organización” contiene estas tres definiciones las cuales contribuyen a nivel de porcentaje total a todo el “PO2” si realizamos el promedio de los tres porcentajes obtenemos el resultado del 66.6666%.

Posteriormente, una vez habiendo obtenido todos los porcentajes de cada proceso, los pasaremos a la matriz “Matriz de Evaluación de Dominio de Procesos COBIT” para posteriormente obtener el porcentaje de satisfacción de los dominios, y a su vez ordenar cada proceso para determinar cuál es el que necesita de la atención por parte del departamento de sistemas.

Cómo se puede observar a continuación:

MATRIZ DE EVALUACION DE DOMINIO DE PROCESOS COBIT	
Proceso	Porcentaje Obtenido
Planificación y Organización	
PO3 Determinar la dirección tecnológica.	100%
PO6 Comunicar los objetivos y direcciones de la gerencia.	88.8888%
PO10 Administrar proyectos.	83.3333%
PO4 Definir la organización y las relaciones de TI.	72.2222%
PO2 Definir la arquitectura de la información.	66.6666%
Adquisición e Implementación	
AI5 Administrar cambios.	94.4444%
AI1 Identificar soluciones automatizadas.	91.6666%
Entrega y Soporte	
ES8 Asistir y asesorar a los clientes.	88.8888%
ES7 Educar y capacitar a los usuarios.	72.2222%
ES1 Definir y administrar niveles de servicio.	66.6666%

Tabla 4. Matriz de Evaluación de Dominio de Procesos COBIT.

Para poder determinar nuestro porcentaje total del modelo COBIT realizamos el promedio de los siguientes valores:

Planeación y Organización	82.2221%
Adquisición e Implementación	93.0555%
Entrega y Soporte	75.9258%

Tabla 5. Resultado Porcentajes de Matriz de Evaluación COBIT.

Entrevista con los responsables del área de sistemas

El siguiente paso para implementar es el uso de las entrevistas diseñadas con el jefe de sistemas, éstas entrevistas se verán enfocadas a la tarea que realiza y los conocimientos con los que debe contar en relación con su ocupación en el puesto de trabajo, así como la manera en la que las actividades se gestionan en el departamento.

Esta información debe ser analizada posteriormente haciendo uso de las nomenclaturas correspondientes para poder hacer una evaluación y ser integrada en el informe.

Para generar un ambiente ideal y evitar la tensión natural a la hora de ejecutar la entrevista (lo cual puede afectar los resultados) se recomienda realizar en dos rondas la actividad y no generar inconsistencias en los itinerarios acordados.

Muchos auditores caen en el error de querer escuchar sólo los problemas. Es de vital importancia desarrollar los aspectos positivos también. Estas áreas deberán ser sondeadas tanto como las negativas, porque el auditor necesita entender en detalle el funcionamiento del sistema de comunicaciones.

La información obtenida a través de una entrevista es más difícil de codificar, analizar e interpretar. Nuestra sociedad está tan acostumbrada a las clasificaciones numéricas que a veces dudamos de la validez de las cosas que no podemos colocar en una escala de este tipo. ¿Cuánta gente tiene que mencionar un problema para que éste sea considerado significativo? Las habilidades interpretativas del auditor se verán puestas a prueba en una situación como ésta.

Algunas veces una persona que ocupa un alto cargo en la organización menciona un problema que nunca nadie ha mencionado antes. Sería arriesgado y hasta tonto dejar de lado esta apreciación, sólo por basarse en referentes numéricos.

Puntualizando que la norma ISO 20000 se estructura en torno a la utilización de procesos integrados para la gestión de los servicios TI, posicionándolos en un modelo de referencia y, estableciendo todo aquello que es obligatorio para la buena gestión de los servicios TI. Estos procesos dan cobertura a las necesidades del ciclo de vida de los servicios.

PORCENTAJE DE ACEPTACION		
Porcentaje de Aceptación ISO 20000	Min. 85%	Max.100%

Porcentaje obtenido por parte de la medición de la norma ISO 20000 del departamento de sistemas de la empresa Mai Kai Tec. S.A de C.V.	88.52%
--	---------------

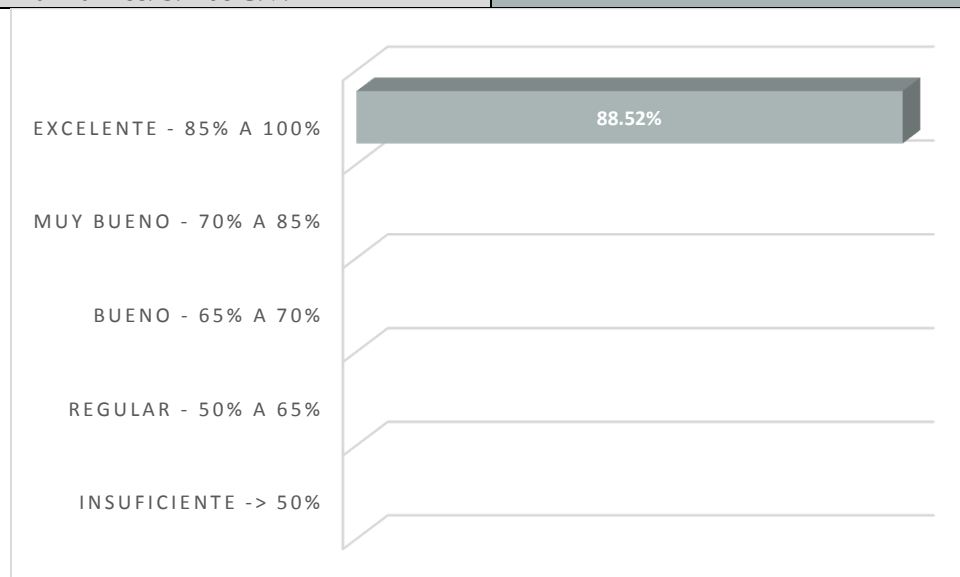


Figura 5..Gráfica de Resultados Entrevista.

3.3 Objetivo 3. Presentar.

3.3.1 Actividad 1. Informe de auditoría.

Descripción de la Actividad..

La elaboración del informe será nuestro archivo que incluirá el ordenamiento de la información, los análisis, los hallazgos y las propuestas de mejora de manera que la empresa pueda entender toda la información recabada acerca de sus procesos y poder dar conclusión a la auditoría realizada.

INFORME DE AUDITORIA

Para el departamento de tecnologías de la información y sistemas computacionales de la empresa:

Mai Kai Tec. S.A de C.V.

Después de haber realizado la inspección correspondiente a:

- a) Procesos de control basados en el modelo COBIT*
- b) Servicios y procesos en base a la norma ISO / IEC 20000*

Se pudieron obtener un grupo de conclusiones y recomendaciones que podrán ser consultadas en el informe de auditoría presentado en esta sección. Este documento incluye el resumen gerencial, estadísticas y evaluaciones obtenidas (ya simplificadas) las cuales justificaran las conclusiones y recomendaciones presentadas a continuación.

INFORME DE AUDITORIA

El objetivo de la auditoria presente es medir la calidad de servicios de TI ofrecidos por el departamento de sistemas. Este objetivo es logrado una vez se haya revisado si los procesos dentro del departamento se basan en una metodología que plantea la norma ISO / IEC 20000 está norma consta de procesos fundamentales para poder ser desempeñada que son los procesos de control, estos procesos deben existir en un ambiente controlado y definido para poder entrar en un modelo PDCA, este modelo refiere a la planeación (Plan), hacer (Do), verificar (Check) y actuar (Act).

Una vez tengamos este ambiente puede entrar en el modelo de gestión de servicio; entonces será cuando la empresa obtenga los fundamentos en su totalidad para ser certificados.

Acerca del Procedimiento de Auditoria

Preauditoria

La auditoría como medida de buenas prácticas y siguiendo una filosofía de trabajo donde se busca la mejora continua, se basó en dos etapas, la etapa de “Preauditoria” que consta de un estudio preliminar de la situación en la que se encuentran los recursos, servicios y estados de TI y la “Auditoria”.

Esta etapa fue un diagnóstico que a su vez nos arrojó una muestra para poder realizar una selección de aquellos procesos que entraron a la auditoría, además que nos ayudó para familiarizarnos con el personal que actúa dentro del organismo.

En base al ordenamiento de la información obtuvimos los siguientes resultados:

A continuación, se presentan las gráficas generales del diagnóstico de los procesos que engloban el modelo COBIT.

INFORME DE AUDITORIA

Información general recabada de la Matriz de Diagnostico – Procesos y Riesgos y Formulario de Entidad

Resultados generales – Etapa de Preauditoria				
Tabla General del Dominio de Planificación y Organización				
Proceso		Puntaje	Porcentaje	Porcentaje Faltante
P8	Asegurar el cumplimiento de los requerimientos externos	4.4722	88.888	11.112
P10	Administrar proyectos.	4.4166	88.332	11.668
P5	Administrar la Inversión de TI.	4.3333	86.666	13.334
P4	Definir la organización y las relaciones de TI.	4.1944	83.888	16.112
P7	Administrar los recursos humanos.	4.0833	81.666	18.334
P3	Determinar la dirección tecnológica.	3.9166	78.332	21.668
P11	Evaluar los riesgos.	3.8888	77.776	22.224
P1	Definir un plan estratégico de TI.	3.8333	76.666	23.334
P6	Comunicar los objetivos y direcciones de la gerencia.	3.7221	74.442	25.558
P9	Administrar la calidad.	3.5000	70.000	30.000
P2	Definir la arquitectura de la información.	3.4444	68.888	31.112

Grafica General de resultados del Dominio de Planificación y Organización

Tabla 6. Tabla General del Dominio de Planificación y Organización.

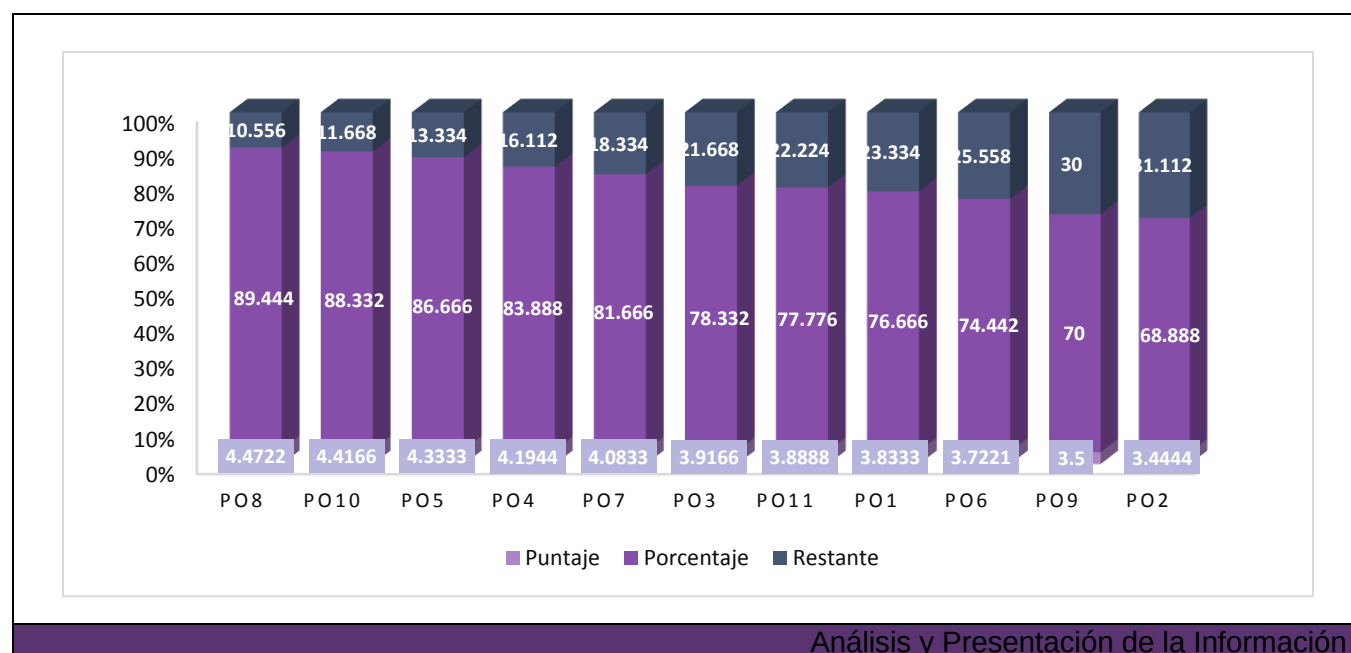


Figura 6. Gráfica de Resultados Tabla General del Dominio de Planificación y Organización.

Fortalezas: Gracias a este análisis podemos observar que los procesos de aseguramiento de los requerimientos externos cumplen un nivel que supera el estándar definido a la evaluación.

La administración de proyectos es un fuerte que de hecho es forzoso, ya que la vanguardia va de la mano con el constante flujo de innovación, mejoras al sistema y frente a los problemas que presenta el mundo informático en la actualidad.

Otro punto a favor de la empresa en el dominio de planificación y organización es el proceso de la administración de la inversión de TI dónde podemos entender que este sea un punto fuerte gracias a la filosofía que sigue la empresa. Los recursos que sostiene y la metodología de inversión hace que la empresa pueda justificar los costos, la capacitación de su recurso humano y genera un plano de seguridad y confianza para sus clientes que son desde los alumnos hasta los padres de familia que deciden acudir a esta institución.

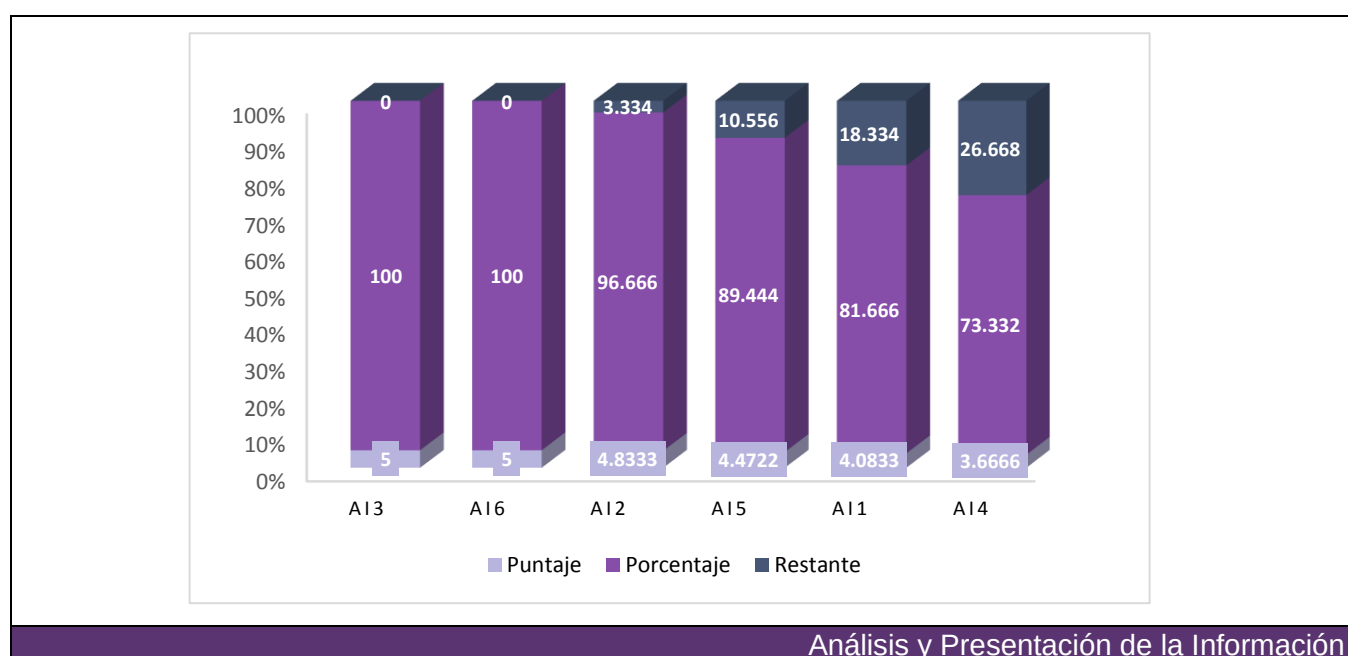
Oportunidades: La oportunidad que tiene el departamento de TI frente al dominio de planificación y organización es que la empresa a la que prestan su servicio está dispuesta a la inversión de mejoras y capacitación a su personal ya que la calidad es una de las insignias del colegio por lo que el plan de inversión para una normalización de procesos y actividades además de contar con el personal capaz y joven hace que la organización tenga buenas bases para la actualización y mejora de sus procedimientos.

Debilidades: Los problemas a los que se enfrenta el departamento de TI en el dominio de planificación y organización son la definición de sus procesos, los cuales deben tener una raíz que sostenga el pilar de los métodos realizados, es verdad que hay procesos que necesitan de una flexibilidad y adaptarse dentro del dominio pero cuando hablamos de una organización que puede presentar en sus métodos algunas bases volátiles entonces nos encontramos con problemas como redundancia de información, problemas en cascada o problemas que nos restan el recurso del tiempo para ser enfocados en tareas que requieran mayor atención por lo que el departamento puede tener una fuga de habilidades al tener los recursos y el potencial para crecer pero no ser aprovechadas de la mejor manera.

Amenazas: La amenaza que se puede vislumbrar lejana en el departamento es que empresas que requieren de la actualización continua o al menos que sean constantes con la innovación y caer en la zona de confort y no definir sus procesos puede provocar que la capacidad y cumplimiento de un departamento se vea afectada por la individualidad y no el equipo o el estándar de un departamento por lo que es importante poder tener definidos nuestros procesos.

Resultados generales – Etapa de Preauditoria				
Tabla General del Dominio de Adquisición e Implementación				
Proceso		Puntaje	Porcentaje	Porcentaje Faltante
A3	Adquirir y mantener infraestructura de tecnología.	5.0000	100	0
A6	Instalar y acreditar sistemas.	5.0000	100	0
A2	Adquirir y mantener software de aplicación.	4.8333	96.666	3.334
A5	Administrar cambios.	4.4722	89.444	10.556
A1	Identificar soluciones automatizadas.	4.0833	81.666	18.334
A4	Desarrollar y mantener procedimientos.	3.6666	73.332	26.668

Tabla 7. Tabla General del Dominio de Adquisición e Implementación.



Análisis y Presentación de la Información

Figura 7. Gráfica de Resultados Tabla General del Dominio de Adquisición e Implementación.

Fortalezas: Este dominio presenta un control formidable ya que se ve que los encargados del departamento están completamente adaptados y preparados para un ambiente de soluciones constantes. La manera en la que ejecutan sus servicios y la relación que tienen con sus recursos de TI hacen que la adquisición e implementación quede satisfecha y sólo haya que puntualizar en estándares mínimos para hacer un servicio optimo.

Oportunidades: La oportunidad que puede manifestar este control que tienen en el dominio es que la implementación de tecnologías no sea un reto sumado a un riesgo, el poder adquisitivo de la empresa y la capacidad de los ingenieros para adoptar nuevas tecnologías hacen que la innovación sea un planteamiento cercano y por ende un escenario ideal para la empresa.

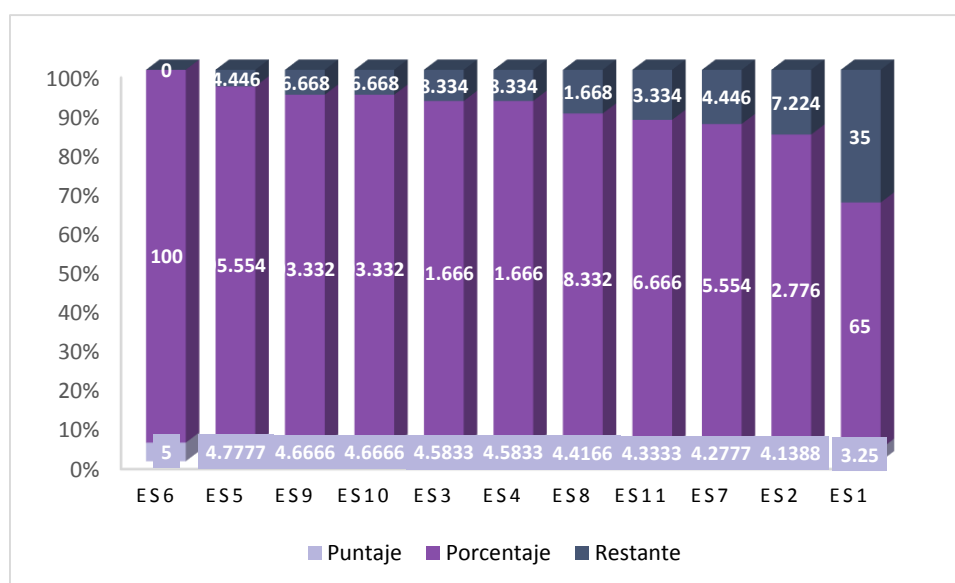
Debilidades: Una de las debilidades del departamento con relación a su adquisición e implementación de tecnología es el tener una pequeña fuga de procesos definidos los cuales cuentan con documentación, pero no es visitada frecuentemente lo que puede generar una evaluación de riesgos poco canalizada. Por otro lado, es una debilidad que se puede controlar con un proceso fijo, definido y que se someta a mediciones constantes, pero no representa un riesgo mayor.

Amenazas: La amenaza puede significar el hecho de no controlar los procesos que tienen ya que esto puede hacer dependientes las soluciones e implementaciones de una tarea individual y no un estándar propuesto por el mismo departamento.

INFORME DE AUDITORIA

Resultados generales – Etapa de Preauditoria				
Tabla General del Dominio de Entrega y Soporte				
	Proceso	Puntaje	Porcentaje	Porcentaje Faltante
E6	Identificar y asignar costos.	5.0000	100	0
E5	Asegurar seguridad de sistemas.	4.7777	95.554	4.446
E9	Administrar la configuración.	4.6666	93.332	6.668
E10	Administrar problemas e incidentes.	4.6666	93.332	6.668
E3	Administrar el rendimiento y la capacidad.	4.5833	91.666	8.334
E4	Asegurar un servicio continuo.	4.5833	91.666	8.334
E8	Asistir y asesorar a los clientes.	4.4166	88.332	11.668
E11	Administrar datos.	4.3333	86.666	13.334
E7	Educar y capacitar a los usuarios.	4.2777	85.554	14.446
E2	Administrar servicios de terceros.	4.1388	82.776	17.224
E1	Definir y administrar niveles de servicio.	3.2500	65	35
Grafica General de resultados del Dominio de Entrega y Soporte				

Tabla 8. Tabla General del Dominio de Entrega y Soporte..



Análisis y Presentación de la Información

Figura 8. Gráfica de Resultados Tabla General del Dominio de Entrega y Soporte

Fortalezas: Con este dominio se puede entender que la empresa tiene un control sobre su entrega y soporte de recursos, servicios y planes de TI. La empresa cubre de manera formidable este dominio, una de las mayores fortalezas es la relación del costo con los recursos y la funcionalidad de estos para poder llevar a cabo la entrega correcta de los recursos a los usuarios.

Oportunidades: La mejor oportunidad de la empresa es el reconocimiento de la mayoría de los usuarios por el nivel de respuesta ante los servicios brindados por esto también es importante destacar que la empresa puede aspirar día con día con mantener la información, los recursos; esto puede ayudar con la formalización y planeación de ciertos procesos la oportunidad de posicionarse como una empresa que pueda funcionar como sede de capacitación para otros planteles hermanos de la institución mayor.

Debilidades: Los problemas a los que se enfrenta el departamento de TI en el dominio de planificación y organización son la definición de sus procesos, los cuales deben tener una raíz que sostenga el pilar de los métodos realizados, es verdad que hay procesos que necesitan de una flexibilidad y adaptarse dentro del dominio pero cuando hablamos de una organización que puede presentar en sus métodos algunas bases volátiles entonces nos encontramos con problemas como redundancia de información, problemas en cascada o problemas que nos restan el recurso del tiempo para ser enfocados en tareas que requieran mayor atención por lo que el departamento puede tener una fuga de habilidades al tener los recursos y el potencial para crecer pero no ser aprovechadas de la mejor manera.

Amenazas: Una amenaza es que al no formalizar los procesos puede demeritar el esfuerzo y conocimiento de los ingenieros ya que pueden depender de un error para disminuir el índice de confianza.

INFORME DE AUDITORIA

Selección de Procesos

Planificación y organización	Puntaje	Indicador	Prioridad
Proceso	Puntaje obtenido	*	ALTA / BAJA
P2 Definir la arquitectura de la información.	4	4	ALTA
P2 Definir la arquitectura de la información.	2.8888	4	
P3 Determinar la dirección tecnológica.	3.3333	4	BAJA
P4 Definir la organización y las relaciones de TI.	4.1666	4	ALTA
P4 Definir la organización y las relaciones de TI.	4.2222	4	
P6 Comunicar los objetivos y direcciones de la gerencia.	3.6666	3	ALTA
P6 Comunicar los objetivos y direcciones de la gerencia.	3.7777	3	
P10 Administrar proyectos.	4.0	4	BAJA
P11 Evaluar los riesgos.	4	3	ALTA
P11 Evaluar los riesgos.	3.7777	3	

Tabla 9. Indicador Tabla General del Dominio de Planificación y Organización..

Adquisición e implementación	Puntaje	Indicador	Prioridad
Proceso	Puntaje obtenido	*	ALTA / BAJA
A1 Identificar soluciones automatizadas.	4.1666	3	ALTA
A1 Identificar soluciones automatizadas.	4.0	3	
A4 Desarrollar y mantener procedimientos.	3	3	BAJA
A5 Administrar cambios.	4.1111	4	BAJA

Tabla 10. Indicador Tabla General del Dominio de Adquisición e Implementación.

Entrega y soporte	Puntaje	Indicador	Prioridad
Proceso	Puntaje obtenido	*	ALTA / BAJA
E1 Definir y administrar niveles de servicio.	3.5	3	ALTA
E1 Definir y administrar niveles de servicio.	3.0	3	
E7 Educar y capacitar a los usuarios.	4.2222	3	BAJA
E8 Asistir y asesorar a los clientes.	4.0	3	BAJA

Tabla 11. Indicador Tabla General del Dominio de Entrega y Soporte.

Por otro lado, se seleccionaron aquellos procesos que presentan una necesidad de ser analizados y entender el funcionamiento e impacto en la empresa y medir su nivel de calidad dentro de los dominios de COBIT e ISO / IEC 20000.

Niveles de Madurez CMMI			
Nivel	Porcentaje mínimo	Porcentaje ideal	Porcentaje de la Org.
Nivel 5	95%	100%	81.3194%
Nivel 4	85%	95%	
Nivel 3	75%	85%	
Nivel 2	65%	75%	
Nivel 1	55%	65%	

Tabla 12. Niveles de Madurez CMMI.

Análisis y presentación de la información:

Nivel 3: Definido. Las actividades de control existen y están diseñadas, han sido documentadas y comunicadas a los empleados, las desviaciones de las actividades de control probablemente no se detecten.

Resultado: La organización cuenta con un nivel de madurez 3.

Evaluación de la Entrevista con el jefe de Sistemas

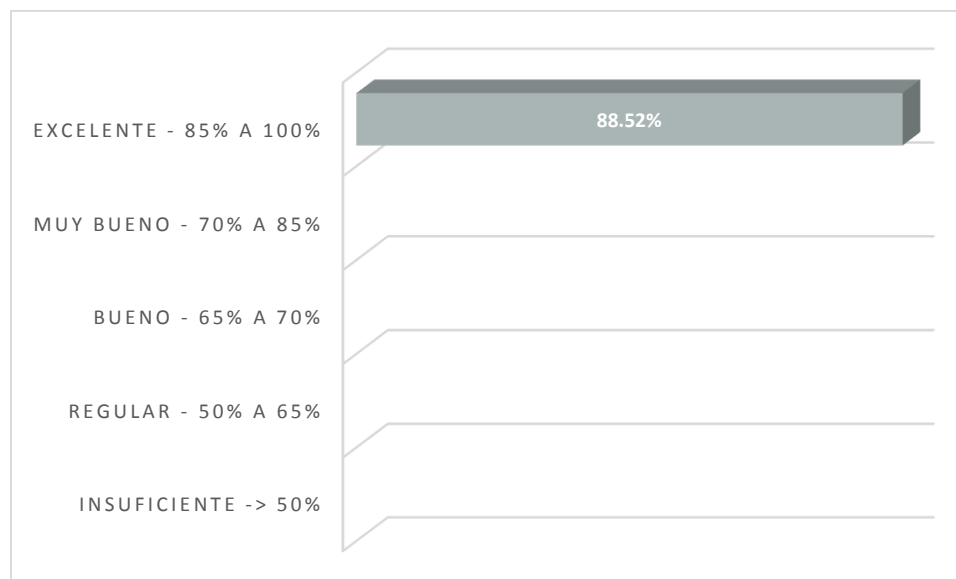
Puntos para mejorar en la información:

Hallazgos y recomendaciones durante la entrevista	
Nomenclatura Gral.	Comentarios
F1-Q4-2	Necesita haber más factores que puedan dificultar la tarea, por lo que me gustaría replantear la respuesta y hacerla más consistente.
F2-Q1-3	Puntualizando en el nivel de satisfacción de un procedimiento, la documentación es una herramienta que permite tener un control sobre acontecimientos por lo que el nivel de logro no puede basarse solamente con información recabada y no registrada.
F2-Q3-2	En cuestión de funcionalidad se puede interpretar que se debe al buen trato y ambiente que existe dentro del departamento, sería aportador complementarlo con un canal o bitácora para tener un control de situaciones.
F2-Q5-3	Para reforzar la confianza de departamentos vecinos a ustedes, podría recomendar tener un control de estructura de la información dentro del área, así como sus procedimientos, mismos que puedan ser compartidos para generar un ambiente de formalidad y por ende aumentar el índice de confianza.
F2-Q7-3	Evaluar las líneas o canales de comunicación para una mejora.
F2-Q8-2	Investigar acerca de mejoras de calidad es el paso siguiente a aquellas instituciones u organizaciones que buscan una mejoría o un mejor posicionamiento de vanguardia ante otras empresas.
F2-Q9-2	El control de acceso puede ser cualquier método de extracción de datos, consulta, solución o algún método que implique que los administradores procedan a una tarea y esté debidamente definida y documentada.
F3-Q3-2	Necesita evidenciar el control de los incidentes mostrando la documentación mencionada.
F3-Q14-3	El diagrama de flujo puede ser opcional, pero es necesario que los pasos sigan una lógica y procedimientos de verdad estén siendo controlados y medidos.
F4-Q9-3	Se requiere de la evidencia que menciona para poder justificar algunos puntos de la fase de la entrevista, pero dado el recurso y operabilidad puede verse evidenciado.

Tabla 13. Hallazgos y Recomendaciones.

Evaluación del cuestionario de aceptación basándose a la norma ISO / IEC 20000

PORCENTAJE DE ACEPTACION		
Porcentaje de Aceptación ISO 20000	Min. 85%	Max.100%
Porcentaje obtenido por parte de la medición de la norma ISO 20000 del departamento de sistemas a la empresa Mai Kai. Tec. S.A de C.V	88.52%	



NOTAS DEL AUDITOR.

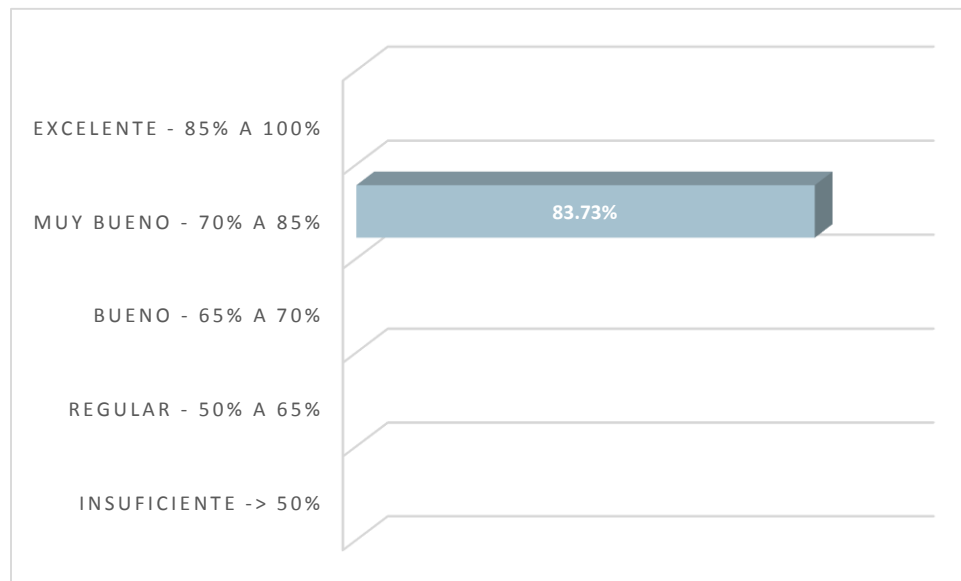
Conclusión: El departamento de TI cuenta con muy buenas bases para poder ser una empresa aspiracional a una certificación ISO, no obstante, esto no quiere decir que los procesos que realizan dentro del departamento sean procesos completamente definidos, por lo que se recomienda canalizar y definir los puntos con el área de control COBIT para poder acceder en un modelo de mejora continua del servicio.

INFORME DE AUDITORIA

Evaluación del cuestionario de aceptación basándose al modelo de control COBIT

PORCENTAJE DE ACEPTACION		
Porcentaje de Aceptación COBIT	Min. 85%	Max.100%
Porcentaje obtenido por parte de la medición de los dominios seleccionados del modelo de control	83.7344 %	

COBIT del departamento de sistemas a la empresa Mai Kai. Tec. S.A de C.V	
---	--



NOTAS DEL AUDITOR.

Conclusión: El departamento de TI necesitará reforzar algunos procesos cuya importancia radica en la definición de sus procesos para poder llevar a cabo unas buenas prácticas, dicho esto el porcentaje faltante es poco por lo que el pequeño ajuste dentro de la organización puede llevarlos a una revisión post auditoria cumpliendo un estándar adecuado para poder certificarse en la norma ISO / IEC 20000.

4. CONCLUSIONES

Como conclusión se puede decir que para lograr la calidad en un proyecto relacionado al desarrollo de software es necesaria la correcta intervención por parte de todos los asociados vinculados a dicho proyecto, ya que cada uno de ellos forma parte importante en el desarrollo y validación del propio proyecto. Esto implica desde el código empleado en la parte del desarrollo del proyecto hasta en las pruebas que se realizaron en cada una de las fases para ir sembrando el correcto desarrollo dentro de estas.

A su vez, por medio de un modelo de trabajo se garantiza la retroalimentación de la información obtenida durante el proceso de pruebas, para dar pie a la solución de errores obtenidos en caso de existir, en el caso particular de este reporte, los errores encontrados a lo largo de la fase de pruebas han ayudado al desarrollo del mismo así como en su implementación en relación a la calidad para asegurar que la empresa tenga resultados óptimos al momento de utilizar el proyecto para fines empresariales.

Así mismo, toda empresa que se encuentre en el rubro de desarrollo y comercialización debe tener contemplada la calidad, y más hoy en día en el cual la sociedad vive en un mundo más globalizado gracias al internet, donde el mercado es cada vez más competitivo. La calidad en un producto no se puede mirar como una opción en los tiempos actuales donde los usuarios y clientes son más exigentes en cuanto a los servicios y productos que consumen de las empresas, y donde una vulnerabilidad puede ser aprovechada para afectar a millones de usuarios o clientes con su información o incluso puedan verse afectadas sus finanzas o de la propia empresa.

5. COMPETENCIAS DESARROLLADAS

1. Coordina y participa en equipos multidisciplinarios para la aplicación de soluciones innovadoras en diferentes contextos.

1.1. Se desarrolló esta competencia debido a que se formó parte de diversos grupos de trabajo con el objetivo de mejorar procesos e implementaciones dentro del proyecto, así como aplicar soluciones prácticas a los errores encontrados dentro de este. A su vez, se pudieron mejorar las habilidades de comunicación para dar a entender ideas o puntos de vista.

2. Diseña, configura y administra redes de computadoras para crear soluciones de conectividad en la organización, aplicando las normas y estándares vigentes.

2.1. En esta competencia, se administró, evaluó y aplico las normas y estándares mencionados ISO 20000-1.

3. Detecta áreas de oportunidad empleando una visión empresarial para crear proyectos aplicando las Tecnologías de la Información y Comunicación.

3.1. Dentro de esta competencia, se presentó la oportunidad de observar y aprender de diversos proyectos que se llevan a cabo dentro de la empresa además de tener una breve idea de lo que es el desarrollo de un proyecto con fines diferentes.

4. Evalúa tecnologías de hardware para soportar aplicaciones de manera efectiva.

4.1 Dentro de esta competencia, siendo parte de la auditoría se evalúa correctamente conforme a la norma ISO 20000

5. Detecta áreas de oportunidad empleando una visión empresarial para crear proyectos aplicando las Tecnologías de la Información y Comunicación.

5.1 Se logra obtener la visión empresarial en el proceso de este reporte en la aplicación de las Tecnologías de la Información.

6. FUENTES DE INFORMACIÓN

- AcademiaLab. (s. f.). Recuperado de <https://academia-lab.com/enciclopedia/historia-de-la-ingenieria-de-sistemas/>
- User, S. (2018, 7 marzo). La Informática. Recuperado de <https://www.informatica.us.es/index.php/conoce-tu-futura-escuela/la-informatica>
- Valenzuela, I. (2019b, junio 19). LA ERA DIGITAL. Agile Scrum. Recuperado 9 de diciembre de 2022, de <https://www.agilescrum.cl/post/la-era-digital>
- Molares, M. C. (2021, 12 julio). Digitalización de procesos: beneficios y pasos a seguir. ASM Soft. Recuperado de <https://asm.es/digitalizacion-de-procesos-beneficios-y-pasos-a-seguir/>
- Ceupe, B. de. (2020, 19 mayo). Tecnologías de la información. Ceupe. Recuperado de <https://www.ceupe.com/blog/que-son-las-tecnologias-de-la-informacion.html>
- Técnica Administrativa ISSN 1666-1680. (2018b, abril 15). Professional profile of the engineers in ITC. Recuperado de <http://www.cyta.com.ar/ta/article.php?id=170201>
- Timetoast. (2018, junio). Antecedentes de Auditoría timeline. Timetoast timelines. Recuperado de <https://www.timetoast.com/timelines/antecedentes-de-auditoria-81fa368e-3609-4eb4-ade3-8e84097b9e5d>
- L.Digital. (2021, 4 enero). Auditoria informática, objetivos, metodología e importancia. Estudia en línea. Recuperado de <https://laedu.digital/2021/09/07/auditoria-informatica-objetivos-metodologia-e-importancia/>
- Galán, C. (2018, 7 agosto). ¿Cuáles son los beneficios de la normalización y la certificación? addalia. Recuperado de <https://blog.addalia.com/los-beneficios-de-la-normalizacion-y-la-certificacion>
- W., M. (2022, 4 agosto). Historia de la ISO - International Standarization Organization. Blog de Calidad ISO. Recuperado de <https://blogs.x.uoc.edu/calidad-iso/historia-de-la-iso/>

- Escuela Europea de Excelencia. (2020, 23 abril). La historia y el futuro de la serie de normas ISO 9000. Recuperado de <https://www.escuelaeuropeaexcelencia.com/2019/06/la-historia-y-el-futuro-de-la-serie-de-normas-iso-9000/>
- Manjaly, S. (2022, 2 septiembre). ISO 20000: todo lo que tienes que saber. Recuperado de <https://blog.invgate.com/es/iso-20000>