UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

AUDITORÍA BASADA EN COBIT 4.1 PARA EL USO ÓPTIMO DE LAS TIC Y LA SEGURIDAD INFORMÁTICA EN LA EMPRESA ARCOPA S.A. PAITA; 2017.

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

AUTORA

BACH. RUTH ARACELLY PANGALIMA ALBÁN

ASESOR

MGTR. EDY JAVIER GARCÍA CÓRDOVA

PIURA – PERÚ

2018

JURADO EVALUADOR DE TESIS Y ASESOR

DR. ING. VÍCTOR ÁNGEL ANCAJIMA MIÑÁN

PRESIDENTE

MGTR. ING. MARLENY SERNAQUE BARRANTES

MIEMBRO

MGTR. ING. OSWALDO GABIEL CORONADO ZULOETA

MIEMBRO

MGTR. EDY JAVIER GARCÍA CORDOVA

ASESOR

DEDICATORIA

A mis padres, porque ellos en todo momento estuvieron a mi lado brindándome su apoyo incondicional, sus consejos para hacer de mí una mejor persona y quienes me impulsan cada día a seguir adelante.

Ruth Aracelly Pangalima Albán

AGRADECIMIENTO

A Dios, por la vida que día a día me concede, por disfrutar cada momento de mi vida y guiarme por el camino que ha trazado para mí, por la fuerza que impone en mí para lograr cada objetivo a lo largo de toda mi vida.

Mi más sincero agradecimiento a la Universidad Católica Los Ángeles de Chimbote, que me abrió las puertas para de llegar a ser un profesional para bien de la comunidad.

Asimismo, agradezco a la Empresa Pesquera ARCOPA S.A de Paita, por concederme la oportunidad de llevar a cabo el proyecto de tesis, brindándome la suficiente información y tiempo para continuar con dicha investigación.

Y mi especial agradecimiento al Mgtr. Ing. Edy Javier García Córdova, Asesor desde el inicio de realizar el proyecto de investigación brindarme sus conocimientos, asesorías, por su paciencia y tiempo dedicado a cada una de mis inquietudes durante el desarrollo de la misma, por su apoyo en la culminación de la presente tesis.

Ruth Aracelly Pangalima Albán

RESUMEN

La presente tesis fue desarrollada bajo la línea de investigación Implementación de las tecnologías de información y comunicación (TIC) para la mejora continua de la calidad en las organizaciones del Perú, de la Escuela Profesional de Ingeniería de Sistemas de la Universidad los Ángeles de Chimbote (Uladech Católica); cuyo objetivo general consistió en Implementar la auditoría basada en COBIT 4.1, para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A; teniendo un diseño de tipo cuantitativo, descriptiva y explicativa, empleando el diseño de investigación no experimental, de corte transversal con un esquema de una sola casilla; trabajando con una muestra de 27 trabajadores asociados en el uso de las TIC; para ello se logró aplicar un conjunto de encuestas orientadas a la medición y control de las variables propuestas para su estudio, obteniendo los siguientes resultados: El 61% de los trabajadores encuestados están satisfactoriamente de acuerdo que al aplicar la Auditoría será de gran beneficio para mejorar la seguridad en cada uno de sus procesos de toda la organización, el 69% de los trabajadores encuestados se encuentran satisfactoriamente de acuerdo que al aplicar la Auditoría será de gran beneficio para mejorar la seguridad en cada uno de sus procesos de toda la organización y el 75% de los trabajadores encuestados están satisfactoriamente de acuerdo que al aplicar la Auditoría será de gran beneficio para mejorar la seguridad en cada uno de sus procesos de toda la organización.

Palabras claves: Auditoría, Seguridad en la organización, Tecnologías de Información y Comunicación.

ABSTRACT

This thesis was developed under the line of research "Implementation of information and communication technologies (TIC) for the continuous improvement of quality in organizations in Peru, of the professional school of Systems Engineering of the Catholic University Los Angeles de Chimbote(Uladech Catholic)"; whose general objective was to implement the audit based on COBIT 4.1, for the optimal use of TIC and computer security in the company ARCOPA S.A; having a design of quantitative, descriptive and explanatory type, using the non-experimental research design, of a cross-section with a single-box scheme; working with a sample of 27 workers associated in the use of ICT; For this purpose, a set of surveys aimed at measuring and controlling the variables proposed for their study were obtained, obtaining the following results: 61% of the workers surveyed satisfactorily agree that applying the audit will be of great benefit to improve security in each of its processes throughout the organization, 69% of the workers surveyed are satisfactorily in agreement that applying the audit will be of great benefit to improve security in each of their processes throughout the organization and the 75% of the workers surveyed satisfactorily agree that applying the audit will be of great benefit to improve security in each of their processes throughout the organization.

Keywords: Audit, Security in the organization, Information and Communication Technologies.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

I. INTRODUCCIÓN

Las Empresas tanto privadas como públicas, actualmente están desarrollando un mayor alcance en la sistematización para cada uno de sus procesos, utilizando herramientas actualizadas, equipo informático y personal capacitado para ejecutar los procesos definidos, para obtener un mayor rendimiento laboral, logrando determinar si los controles implementados son eficientes y suficientes, identificando causas de los problemas que existen en las entidades ya sean sistemas de información, redes, brindando soluciones a problemas específicos de las TIC, con acciones preventivas y correctivas necesarias para mantener a las tecnologías informáticas confiables y disponibles.

En su totalidad muchas de las Empresas no le dan importancia de realizar auditorías basadas en marcos de referencia, manteniendo una idea errónea de que este tipo de herramienta no les corresponde y lo perciben como un gasto y no como una inversión; es por eso que esta perspectiva es básica y necesaria como es el de una auditoría en el uso óptimo de las TIC y la seguridad informática.

COBIT 4.1, es un marco referencia que permite el control de todos los aspectos técnicos y riesgos de negocios, habilitando el desarrollo de políticas claras y buenas prácticas para el control de TIC a lo largo de las organizaciones, estableciendo los criterios técnicos a implementar o controlar para el manejo de la seguridad informática, promoviendo la competitividad en las Empresas a partir de la implantación de una cultura de gestión, seguridad y calidad para afrontar las demandas de su sector, mejorando sus procesos con la garantía del aumento de la seguridad de sus sistemas de información y de las comunicaciones.

La presente investigación propone la Implementación de una auditoría para el uso óptimo de las TIC y la seguridad informática con la finalidad de medir los riesgos y evaluar los controles para el uso de las tecnologías de información, haciendo uso de técnicas y estrategias de análisis, que permitan una alta gestión de tecnologías de

información, a disposición de las empresas, para lograr apoyar a las empresas u organizaciones al éxito del negocio, es por esta razón que el departamento tecnológico de la Empresa ARCOPA S.A, ha llevado un estudio acerca de cada uno de sus procesos que realizan las TIC Y procedimientos de seguridad Informática, ocasionando retrasos en las diversas operaciones que realiza la misma, en la que casi su totalidad fluye por canales de redes, por lo cual necesitan verificar las vulnerabilidades y mejoras en sus operaciones, como también contar con procedimientos de seguridad y controles en caso de contingencias, entre otros.

Así mismo, la Empresa donde se desarrolla el presente trabajo de investigación, ARCOPA S.A, ha venido tratando diferentes enfoques con respecto al uso de las TIC apoyadas a la seguridad informática; alcanzando encontrar la siguiente situación problemática, la cual indicaremos a continuación, especificando las causas que ocasionan aquellos problemas:

1. Existe un alto grado de inseguridad en el uso de sus aplicaciones, esta inseguridad está reflejada en varios aspectos como por ejemplo: desactualización de equipos, ausencia de políticas de seguridad.

2. El tiempo de espera en los servicios informáticos y uso de sus aplicaciones.

3. Algunos equipos de cómputo con los que cuenta la Empresa están desactualizados. Así mismo, en cuanto al mantenimiento del mismo se realizan anualmente. La causa es que no existe una política adecuada de actualización periódica, generando deficiencias y vulnerabilidades en su uso.

4. El personal no está capacitado en el uso de las nuevas tecnologías y aplicaciones en informática, limitando el conocimiento primordial de cada usuario.

5. En los mecanismos de seguridad para las aplicaciones y los sistemas, conocidos Antivirus están desactualizados.

6. En cuanto a las acciones o actividades, ante posibles problemas e inconvenientes que puedan presentarse en los servidores donde se maneja la información de la Empresa, se tienen que contactar con terceras personas para solución de fallas, estando propensos a robos de información.

7. No hay un conocimiento de Políticas de seguridad, estrategias y niveles de riesgo de las TIC.

8. Se suelen presentar fallas de seguridad, problemas con la información, en cuanto a la disponibilidad, integridad, etc.

9. No se proporciona un control efectivo sobre sus recursos y operaciones.

10. No se evalúan ni identifican los puntos débiles de las TIC.

11. Los usuarios no están al día en cuanto a la tecnología y su seguridad.

En base a la problemática descrita en los párrafos anteriores, se desarrolla el siguiente enunciado del problema: ¿De qué manera beneficia la auditoría basada en COBIT 4.1, para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A.?

Dando respuesta a la problemática, se ha planteado el siguiente objetivo general: Implementar la auditoría basada en COBIT 4.1, para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A., implicando con ello los siguientes objetivos específicos:

1. Incrementar el nivel de seguridad de los procesos de TIC de la Empresa ARCOPA S.A.
2. Capacitar al personal involucrado en TIC sobre la seguridad informática.

3. Analizar, evaluar y diagnosticar la situación actual con respecto a los marcos de referencia y control interno para obtener un sistema que permita crear un ambiente seguro de las TIC.

La presente investigación encuentra su justificación operativa, porque permitir obtener un conjunto de estrategias y metodologías para el buen manejo de la información y de las TIC, ofreciendo un mayor control en su seguridad, contando con procedimientos electivos que permitan afrontar cualquier eventualidad, brindando a la Empresa fiabilidad, confiabilidad, eficiencia, eficacia y seguridad en todas sus operaciones.

Es justificable tecnológicamente, ya que al implementar la auditoría basada en COBIT 4.1, para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A., adquiere gran importancia ya que se pretende identificar y describir los factores que afectan en la seguridad del servicio informático de la Empresa, mejorando el uso de la información y procesos actuales, para un buen desempeño de todos sus trabajadores en cada una de sus actividades, contribuyendo al direccionamiento de buenas prácticas y conocimiento primordiales de las TIC a un nivel aceptable por la Empresa.

Económicamente se justifica por la razón que al implementar una auditoría basada en COBIT 4.1, para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A., ayudará a mejorar cada uno de los procesos de toma de decisiones dentro de los procesos de TIC, llegando a reducir costos y ahorro de tiempo, ya que mediante ella disminuye el impacto de riesgos probables en redes, información, equipos y procesos, asimismo permite que el manejo de Seguridad de las TIC sea más fructífero y en menos tiempo.

II. REVISIÓN DE LA LITERATURA

2.1. Antecedentes

2.1.1. Antecedentes a Nivel Internacional

Actualmente, Ecuador cuenta con un marco regulatorio y normativo reducido en materia informática; es por ello que las normas y organizaciones internacionales más relevantes en este ámbito no han sido objeto de análisis, sino que se ha tomado como referencia para el estudio realizado. Las organizaciones más importantes son: The Institute of Internal Auditors (IIA), e Information System Audit and Control Association (ISACA) (1).

En la tesis sobre la Evaluación del cumplimiento de las normas técnicas para la gestión y control de las tecnologías de información en la organización de Curridabat, Costa Rica; se reconoce un rol vital de TI en el alcance de los objetivos de la Organización e incluso la situación adquiere mayor relevancia cuando la institución enfrenta una mayor demanda por servicios de calidad en la atención de clientes internos y externos, sin embargo, el estado actual de la gestión de no necesariamente asegura el mejor resultado ni la mejora continua de los procesos. Los procesos y procedimientos asociados a la prestación de servicios de TI, deben estar centrados en objetivos cuantificables, que conduzcan al Departamento, de forma alineada con la Institución, hacia los resultados esperados.

Como consecuencia del desarrollo de este proyecto bajo los términos de alcance definidos, es de esperar como beneficios directos un aumento en la productividad del Departamento, se establece una fuente única para el alineamiento de la gestión de TI y sus responsabilidades respecto de planes y objetivos de la organización y se optimiza el desempeño, se aprovechan los

procesos de acuerdo a las mejores prácticas del mercado y se puede incrementar significativamente la productividad de la planificación (2).

Villegas Marianella, en el año 2009 (3), en su artículo: "Modelo de Madurez de la Gestión de la Seguridad Informática en el contexto de las Organizaciones Inteligentes", ofrece una propuesta de un modelo de madurez para la Gestión de la Seguridad de la Información partiendo del punto de vista de las Organizaciones Venezuela Inteligentes, las cuales se enmarcan en cinco disciplinas: el dominio personal, los modelos mentales, la visión compartida, el aprendizaje en equipo y el pensamiento sistémico. El modelo está integrado por 5 niveles: Inicio, Crecimiento, Desarrollo, Madurez Organizacional e Inteligencia Organizacional. Con ello se busca disminuir la complejidad y la incertidumbre en la gestión de la seguridad de la Información en las organizaciones lo que contribuirá a la fácil identificación de las herramientas de hardware y software para proteger los activos informáticos. Para desarrollar este artículo los autores realizaron una investigación de tipo exploratorio a través de entrevistas estructuradas a personal experto, asesores de Empresa, profesores del área de seguridad, revisión de textos, sitios web entre otros. Los autores han desarrollado diferentes artículos sobre temas relacionados por lo que cuentan con experiencia en el campo. La bibliografía utilizada es diversa y es de destacar que incluyen otros artículos desarrollados por los mismos autores.

2.1.2. Antecedentes a Nivel Nacional

Santos Llanos y Daniel Elías (4), en el año 2016, en su Tesis “Establecimiento, Implementación, Mantenimiento y Mejora de un Sistema de Gestión de Seguridad de TI, Basado en COBIT 5, para

una Empresa de Consultoría de Software", determinaron que un Sistema de Gestión de TI, el cual cuenta con un marco formal de requisitos a cumplir, permitirá que los directivos y demás involucrados gestionen y tomen decisiones adecuadas respecto a la seguridad de información de la organización, para asegurar que cuente con niveles adecuados respecto a la confidencialidad, integridad y disponibilidad de la información crítica que se maneja como parte de su operación. Este modelo permite que el sistema opere bajo un principio de mejora continua, que beneficia permanentemente a la organización, propiciando un manejo adecuado de la seguridad de su información y Tecnologías.

Alva (5), en el año 2011, en su tesis: "Las Tecnologías de información y comunicación como instrumentos eficaces en la capacitación a maestristas de educación con mención en Docencia en el Nivel Superior de la Universidad Nacional Mayor de San Marcos, Lima, Perú". La Investigación fue de diseño no experimental y de tipo descriptivo correlacional. Se obtuvo los siguientes resultados: Las tecnologías de información y comunicación, en lo pedagógico y en gestión del maestrista, influye como instrumento eficaz en la capacitación de los maestristas de la Facultad de Educación, con mención en Docencia en el Nivel Superior, de la Universidad Nacional Mayor de San Marcos.

Vera (6), en el año 2010, en su tesis para la obtención del Grado de Magíster: Competencia en tecnologías de información y comunicación en docentes del área de comunicación de Instituciones educativas de la región Callao, Perú, determinó el diseño cuantitativo no experimental, de tipo descriptivo cuyo problema principal fue ¿Cuál es el nivel de competencia en tecnologías de la comunicación y la información de los docentes del área de comunicación? se planteó como objetivo establecer el

nivel de competencia en tecnologías de la información y la comunicación por parte de los docentes del área de comunicación de las instituciones educativas públicas de secundaria de las Redes Educativas N° 01, 02, 07 y 10 de la región Callao. Se concluyó que el 42% de los docentes encuestados del área de comunicación se encuentra en el nivel medio en cuanto a la dimensión nivel de conocimiento en TIC, lo que equivale a decir que los docentes están adquiriendo mayor conocimiento de las TIC en el diseño y evaluación de experiencias de aprendizaje que incorporen el uso de las TIC, las capacidades, las habilidades y actitudes de sus estudiantes. El 32% de los docentes usan las TIC normalmente, pero el otro 30% lo usa de vez en cuando, lo cual significa que aún están en proceso de mejorar su práctica profesional en TIC. El 46% de los docentes se encuentra en desacuerdo frente a las potencialidades de las TIC, lo cual significa que existe una actitud negativa del docente ante las TIC.

Choque R. (7), en el año 2009, en su tesis doctoral: Estudio en aulas de innovación pedagógica y desarrollo de capacidades TIC en los estudiantes de educación secundaria de la Red Educativa N° 11de la UGEL de San Juan de Lurigancho, Lima, Perú. La investigación fue de diseño casi experimental, por lo que se obtuvo los siguientes resultados: Se confirmó la hipótesis general, que el estudio en las Aulas de Innovación Pedagógica mejora el desarrollo de capacidades TIC en los estudiantes de educación secundaria, frente al desarrollo de capacidades TIC convencionales. Asimismo, la verificación de las hipótesis fue hecha aplicando el T de Student, concluyendo que el estudio en las Aulas de Innovación Pedagógica mejora el desarrollo de capacidades TIC, puesto que los estudiantes en contacto con las nuevas TIC como la computadora y el Internet tienen efectos en su capacidad de su intelecto humano, puesto que

aprenden de la tecnología ciertas capacidades tecnológicas que son cambios permanentes que se dan en los estudiantes.

2.1.3. Antecedentes a Nivel Local

No se han encontrado antecedentes de estudios similares a nivel local.

2.2. Marco teórico – conceptual

Auditoría

De acuerdo a López J., Zuluaga A. (8), la palabra Auditoría proviene del latín auditorius, y de esta proviene la palabra auditor, consiste en evaluar todas las funciones y el control en todas áreas de la organización, indicando la manera objetiva de evaluar la eficacia eficiencia, detectando errores, irregularidades, riesgos, también la seguridad frente al trabajo que realiza la organización, para determinar el soporte adecuado a los objetivos y metas de la organización, para establecer claramente sus funciones, responsabilidades y objetivos. Para ello se ha tomado una variedad de conceptos sobre auditoría:

Según Tamayo y Fabián (8), la auditoría es el examen organizado de una situación, proceso u organización, en materia de calidad, realizado en cooperación con los interesados para verificar la concordancia de la realidad con lo preestablecido y la adecuación al objetivo buscado.

La auditoría es el proceso de verificación sistemática y documentada, cuyo propósito es obtener y evaluar, de forma objetiva, evidencias que permitan determinar si el objeto de la auditoría se ajusta a unos requisitos especificados (9).

Clasificación de auditorías

Auditoría de sistemas de información

Es un examen y validación del cumplimiento de los controles y procedimientos utilizados para la confidencialidad, integridad y disponibilidad de los sistemas de información. Realizada por personal externo a la empresa, proporciona al negocio una evaluación independiente y objetiva de los hechos que, en ocasiones es difícil de obtener cuando se está inmerso en la operación y en presión de la problemática del día a día (10).

Auditoría de renovación

Tiene su concepción después de una Auditoría inicial. El resultado es la emisión de un nuevo certificado que contiene el periodo en que esta se debe volver a llevarse a cabo. Prestando atención especial a las no conformidades detectadas durante la Auditoría inicial, así como la eficacia y grado de implementación de las acciones correctivas y preventivas (11).

Auditoría de Gestión Empresarial

Es una evaluación objetiva, concreta e integral de las actividades que realiza un área o una empresa para cumplir sus fines y objetivos. Esta auditoría examina en forma detallada cada aspecto operativo de la compañía por lo que en la determinación del alcance se debe considerar: logro de los objetivos de institucionales, estructura organizativa, participación individual de cada empleado, verificación del cumplimiento de la normatividad general y específica, evaluación de la eficiencia y economía, medición del grado de confiabilidad de la información financiera y atención a la existencia de procedimientos ineficaces o más costosos (12).

La auditoría de gestión cuenta con un enfoque integral por ello se considera una auditoría de economía y eficiencia.

La gestión comprende todas las actividades de una empresa que implica establecimiento de metas y objetivos, así como la evaluación de su desempeño y cumplimiento de una estrategia operativa que garantice la supervivencia y crecimiento de la misma.

Puntos claves considerados en este tipo de auditoría, según (12):

- La eficacia mide el cumplimiento de los objetivos, esta evaluación permite saber si los programas deben continuarse o no.
- La economía mide las condiciones en que una determinada empresa adquiere los recursos humanos, financieros y materiales.
- La eficiencia es la capacidad de alcanzar un objetivo que nos permite conocer el rendimiento del servicio prestado y la comparación de dicho rendimiento como norma establecida.

Tipos y clases de auditorías informáticas

Auditoría informática de explotación:

- La Auditoría de explotación es el control que se realiza sobre las funciones del Sistema de Información para asegurar que las mismas se efectúen de forma regular, ordenada y que satisfagan los requisitos empresariales. La Explotación Informática se ocupa de producir resultados informáticos de todo tipo: listados impresos, archivos soportados magnéticamente, órdenes automatizadas para lanzar o modificar procesos industriales, etc (13).

Auditoría informática de desarrollo de proyectos o aplicaciones

- Es evaluar la efectividad de los controles existentes y sugerir nuevos controles con el fin de minimizar riesgos y fortalecer el control de dichas aplicaciones

- Ejemplo: se puede aplicar para Controlar los ingresos de datos o proyectos que estos no tengan algunos posibles errores en la digitación, Ingresos de datos incompletos, repetidos u omisiones. Porque se presentan muchos riesgo que deben ser eliminados los fallos de cualquiera de los elementos que intervienen en el proceso informático que amenazan la confidencialidad e integridad de la información de los sistemas de la empresa por una mala metodologías utilizadas en esta (13).

Auditoría informática de sistemas

- Analizar la actividad que se conoce como Técnica de Sistemas en todas sus facetas como son los Sistemas operativos, los Software básico, Software de teleproceso, Optimización de los sistemas y subsistemas y la Administración de base de datos (13).

Auditoría informática de comunicaciones y redes

Consiste en el análisis del entramado conceptual que constituyen las redes nodales, líneas, concentradores, multiplexores, redes locales, etc., no son sino el soporte físico-lógico del tiempo real. En este caso es normal que el auditor requiera de especialistas o expertos en comunicaciones y redes (13).

Auditoría de la seguridad informática

- La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica:

  La seguridad física se refiere a la protección del hardware y de los soportes de datos, así como los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc. Igualmente, a este ámbito pertenece la política de seguros.

La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

- Se verifica las normas y procedimientos requeridos para minimizar las causas de riesgos en los programas computacionales y los datos, en todo el ámbito del Sistema: usuarios, instalaciones, equipos (13).

Auditoría de la Seguridad informática (14)**:**

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos. Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus. El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc (14)**:**

La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

La seguridad informática se la puede dividir como Área General y como Área Específica (seguridad de Explotación, seguridad de las Aplicaciones, etc.). Así, se podrán efectuar auditorías de la Seguridad Global de una Instalación Informática, Seguridad General y auditorías de la Seguridad de un área informática determinada Seguridad Especifica (14)**:**

El sistema integral de seguridad debe comprender (14):

- Elementos administrativos
- Definición de una política de seguridad
- Organización y división de responsabilidades
- Seguridad física y contra catástrofes (incendio, terremotos, etc.)
- Prácticas de seguridad del personal
- Elementos técnicos y procedimientos
- Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.
- Aplicación de los sistemas de seguridad, incluyendo datos y archivos
- El papel de los auditores, tanto internos como externos
- Planeación de programas de desastre y su prueba.

La decisión de abordar una Auditoría Informática de Seguridad Global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida. Se elaboran "matrices de riesgo", en donde se consideran los factores de las "Amenazas" a las que está sometida una instalación y los "Impactos" que aquellas puedan causar cuando se presentan (14)**.**

La Auditoría enfocada a las TIC

La Auditoría de Gestión a las Tecnologías de Información y Comunicaciones, consiste en el examen de carácter objetivo (independiente), crítico (evidencia), sistemático (normas) y selectivo (muestral) de las políticas, normas, funciones, actividades, procesos e informes de una entidad, con el fin de emitir una opinión profesional (imparcial) con respecto a: eficiencia en el uso de los recursos informáticos, validez y oportunidad de la información, efectividad de los controles establecidos y la optimización de los recursos tecnológicos. Este enfoque es totalmente compatible con las prácticas y controles contenidos en COBIT, ITIL, estándares o normativa que relaciona el enfoque COSO, SAC, NIAS, entre otros, que hacen referencia a las pistas de auditoría en los sistemas informáticos, controles de acceso a los sistemas, bases de datos, Áreas de Tecnología de la Información y Comunicaciones (TIC´s) área de servidores, codificación de la información, prevención de virus, fraude, detección y mitigación de intrusos, entre otros; estos estándares no proporcionan un criterio legal aplicable si no han sido adoptados por la entidad, pero sí procedimientos de auditoría para examinar la gestión tecnológica en las diferentes organizaciones del sector público (15).

La auditoría a las TIC (Tecnologías de Información y las comunicaciones) (16), está basada en una evaluación objetiva, selectiva, crítica y sistemática de las políticas, procesos, normas, funciones, actividades de la empresa con el fin de generar un informe del uso eficiente de los recursos informáticos, de la comunicación, la oportunidad en la entrega de la información, aprovechamiento de los recursos y la efectividad de los controles establecidos por el área de Tecnología al interior de la empresa.

Para obtener óptimos resultado durante la ejecución de la auditoria el auditor de TIC debe contar con un conocimiento pleno frente a las Tecnología y Comunicaciones para que pueda tener claridad en los criterios al momento de planear y desarrollar la auditoría al interior de la empresa y hacer uso de su

experiencia para dar un enfoque adecuado y obtener con esto los objetivo planteados al momento de programar la realización de la auditoría de TIC (16).

Al momento de elegir el auditor, este debe contar con la capacidad de implementar procedimientos a través de los cuales se pueda hacer una rigurosa verificación de los recursos tecnológicos y de comunicación, la confidencialidad, integridad, disponibilidad, y confiabilidad de la información que es generada mediante los programas que se ejecutan de manera automática, buscando garantizar los resultados que serán entregados en el informe de auditoría donde los administradores y directivos podrán contar con una medición más exacta de la eficiencia y eficacia de la tecnología y la comunicación al interior de la empresa (16).

COBIT 4.1

La necesidad del aseguramiento del valor de TI, la administración de los riesgos asociados a TI, así como el incremento de requerimientos para controlar la información, se entienden ahora como elementos clave del Gobierno Corporativo. El valor, el riesgo y el control constituyen la esencia del gobierno de TI. El gobierno de TI es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan que TI en la Empresa sostiene y extiende las estrategias y objetivos organizacionales (17).

La evaluación de la capacidad de los procesos basada en los modelos de madurez de COBIT es una parte clave de la implementación del gobierno de TI. Después de identificar los procesos y controles críticos de TI, el modelo de madurez permite identificar y demostrar a la dirección las brechas en la capacidad. Entonces se pueden crear planes de acción para llevar estos procesos hasta el nivel objetivo de capacidad deseado (17).

COBIT ("Control Objectives for Information and related Technology").

"Es el marco aceptado internacionalmente como una buena práctica para el examen de la información, TI y los riesgos que conllevan. COBIT se manipula para efectuar el gobierno de IT y corregir los controles de IT. Contiene objetivos de control, directivas de aseguramiento, medidas de desempeño y resultados, factores críticos de éxito y modelos de madurez" (18).

Para ayudar a las organizaciones a reparar con éxito los retos del negocio, el IT Governance Institute (ITGI) ha publicado la versión de COBIT 4.1 (18).

- COBIT es un framework de Gobierno de TI y un vinculado de instrumentos de soporte para la administración de T.I. que les consiente a los gerentes resguardar la grieta entre las obligaciones de revisión, los aspectos técnicos y peligros de negocio.
- COBIT hace permisible el progreso de una estrategia clara y las buenas habilidades para las revisiones de T.I. a través de las distribuciones de la organización.
- COBIT acentúa en la aprobación a ordenaciones, apoya a las organizaciones a desarrollar el coste alcanzado desde la TI, admite el alineamiento y resuelve la ejecución de la estructura COBIT (18).

Estructura:

Planificación y organización (PO): Habilidades y tácticas. Nivelar la manera en que TI pueda favorecer de la superior manera al logro de los equitativos del negocio (18).

a) Técnica de informática alineado al Plan Estratégico de la organización
b) Métodos de proyectos.
c) Procedimiento de seguridad

d) Método de continuidad de Negocio
e) Procedimiento de Capacitación
f) Regla de Licenciamiento de Software
g) Régimen de mantenimiento preventivo y correctivo
h) Plan de Calidad
i) Cálculos
j) Distribución Organizacional
k) Patrimonios Disponibles
l) Técnicas de trabajo (18).

Adquisición e Implementación (AI) (19)**:** Caracterización de recursos, mejora o adquisición, cambios y/o sustentación de sistemas existentes.

a) Intereses de TI y afines: equipos de cómputo, equipos de red, licencias de software, sistema de información, etc.
b) Propuestas tecnologías
c) Propuestas financieras
d) Estimaciones de distribuidores
e) Estipulaciones
f) Mejora de TI de base
g) Mejora de sistemas de información
h) Desempeño de metodologías y protocolo respectiva.

Entregar y Dar Soporte (DS) (2)**:** Cubre el desembolso de los servicios pretendidos. Incluye la asistencia del servicio, la gerencia de la seguridad y de la persistencia, el poste puntual del servicio a los usuarios, el gobierno de los datos y de las instalaciones estratégicos.

a) Trasmisión de servicios de Desarrollo e Implantación de SI.
b) Apreciación de posibles procedimientos de lo desarrollado o comprado e implantado
c) Medidas de Seguridad

d) Nivel de complacencia de los beneficiarios con relación al servicio otorgado
e) Transmisión de servicios de Soporte Técnico
f) Construcción de TI: Hardware y Software de Base, así como servicios relacionados.

Monitorear y Evaluar (ME) (2)**:** Todos los métodos de TI deben valorar de carácter regular en el tiempo en cuanto a su calidad y desempeño de las amonestaciones de control. Este mando abarca el gobierno del ocupación, el monitoreo del examen interno, el desempeño regulatorio y la concentración del gobierno.

a) Alcance de los planes
b) Estimación interna del desempeño
c) Alegaciones o acreditaciones autónomas de control y seguridad
d) Suministro de auditoría independiente

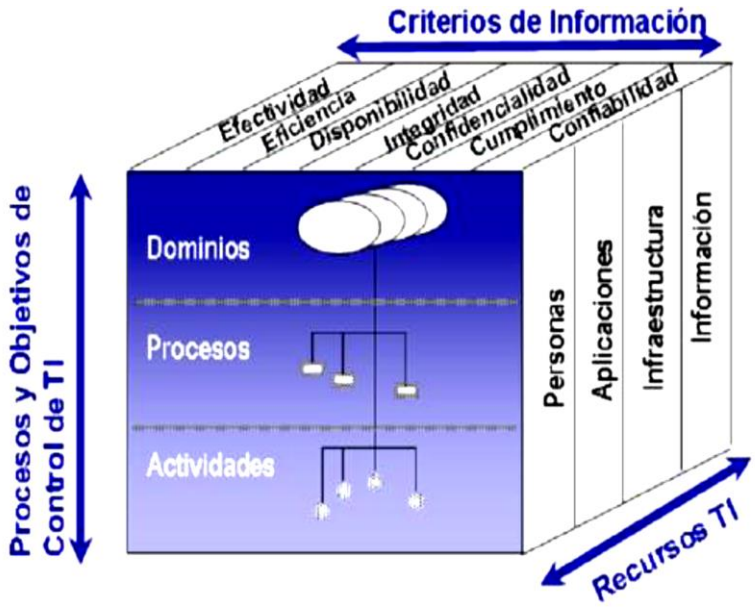
Criterios de Información y recursos de TI según COBIT:

Para integrar los objetivos del negocio, la información necesita "concordar con ciertos criterios a los que COBIT hace referencia como requerimientos de negocio para la información". Al establecer la lista de requerimientos, COBIT acuerda los manuales comprendidos en los modelos referenciales efectivos y populares (2):

- Efectividad: Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
- Eficiencia: Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
- Confidencialidad: Se refiere a la protección de información sensible contra divulgación no autorizada.

- Integridad: Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
- Disponibilidad: Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
- Cumplimiento: Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.
- Confiabilidad de la información: Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento (2).

Figura N° 1: Criterios y Recursos



Fuente: IT Governance Institute (18).

Los recursos de TI identificados en COBIT pueden identificarse/definirse como se muestra a continuación:

- Datos: Los elementos de datos en su más amplio sentido (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.

- Aplicaciones: Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.
- Tecnología: La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc.
- Instalaciones: Recursos para alojar y dar soporte a los sistemas de información.
- Personal: Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, soportar y monitorear servicios y sistemas de información.

Modelo genérico de madurez

0 – No Existente: Escasez completa de cualquier paso reconocible. La Empresa no ha registrado por lo menos que existe una dificultad a solucionar.

1 – Inicial: Consta evidencia que la Empresa ha examinado que las dificultades existen y demandan ser resueltos, Sin embargo; no coexisten métodos de prueba en su lugar existen guías ad hoc que tienden a ser diligentes de forma individual o caso por caso.

2 – repetible: Se han perfeccionado los métodos hasta el punto en que se siguen instrucciones similares en otras áreas que cumplen la misma tarea. No hay preparación o declaración formal de las programaciones estándar, y se deja el encargo al individuo.

3 – Definido: Las instrucciones se han normalizado y argumentado, y se han público a través de adiestramiento. Sin embargo, se deja que el sujeto decida estas técnicas, y es poco probable que se detecten desorientaciones. Las operaciones en sí no son sofisticadas pero determinan las experiencias positivas.

4 – Administrado: Es posible monitorear y medir el desempeño de las programaciones y tomar equilibradas medidas cuando los métodos no estén trabajando de forma positiva. Los términos están bajo invariable

perfeccionamiento y facilitan buenas habilidades. Se usa la sistematización e instrumentos de una manera definida o fraccionada.

5 – Optimizado: Las técnicas se han refinado hasta un nivel de excelente práctica, se asientan en las secuelas de progresos continuos y en un modelo de conocimiento con otras Sociedades. TI emplea de manera formada para motorizar el flujo de compromiso, ofreciendo instrumentales para optimizar la eficacia y la efectividad (2).

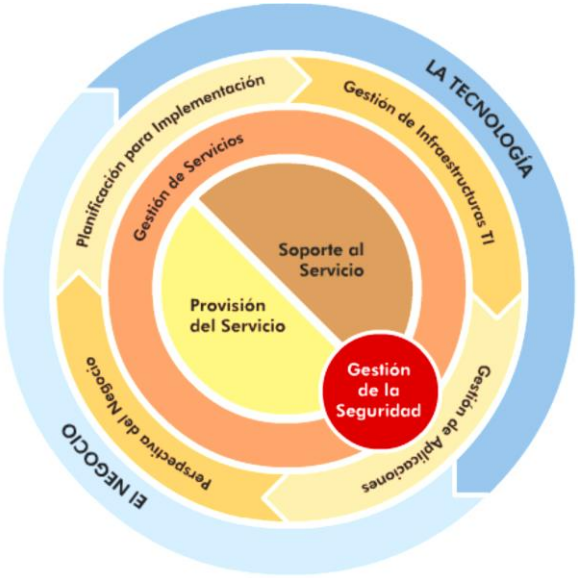
Figura N° 2: Modelo Genérico de Madurez

Fuente: IT Governance Institute (18).

ITIL

ITIL fue perfeccionada al mostrarse de acuerdo que las organizaciones dependen "cada vez más de la Informática para alcanzar sus objetivos corporativos. Esta dependencia en aumento ha dado como resultado una necesidad creciente de servicios informáticos de calidad que se correspondan con los objetivos del negocio, y que satisfagan los requisitos y las expectativas del cliente". A través de los años, el énfasis pasó de estar sobre el perfeccionamiento de las concentraciones de TI a la tarea de servicios TI. La concentración TI (a veces nombrada como un sistema de información) sólo "contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por los procesos de mantenimiento y operaciones" (20).

Figura N° 3: Fundamentos de la Gestión de TI



Fuente: ITIL- Gestión de Servicios TI- Consultora Osiatis (21).

ITIL® (22), es un marco de trabajo público que describe las mejores prácticas en la gestión de Gestión de Servicios de TI (ITSM). De hecho, es el marco de trabajo más utilizado en el mundo para la ITSM, proporcionando un marco para el gobierno de TI, y la gestión y control de los servicios de TI. En definitiva, es un conjunto de procesos que agrupados bajo una estructura lógica, permite a una organización Gestionar sus Servicios de TI de la mejor forma, según la experiencia de una serie de organizaciones que se ha demostrado que lo hacen muy bien.

ITIL® es adoptado porque permite (23):

- Entregar valor a los clientes a través de servicios.
- Integrar la estrategia para servicio con estrategia de negocio y necesidades de clientes.
- Medir, monitorear y optimizar servicios de TI y el desempeño del proveedor de servicios.
- Gestionar la inversión y presupuesto destinado a TI.

• Gestionar el riesgo.

• Gestionar el conocimiento.

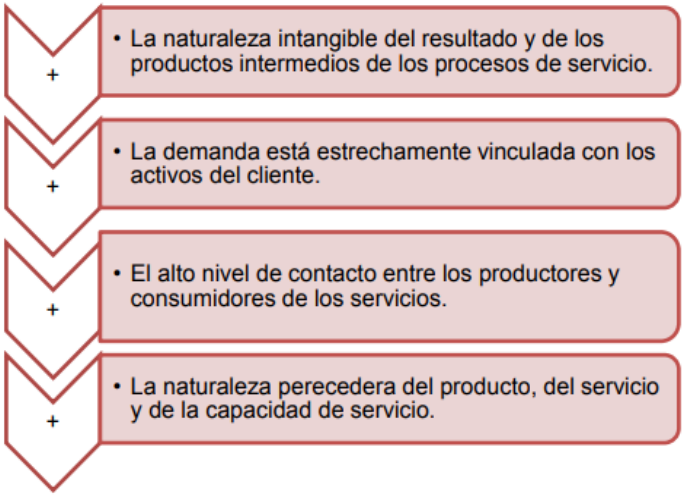
• Gestionar las competencias y recursos para entregar servicios efectivos y eficientes.

• Permitir la adopción de un enfoque estándar para gestionar el servicio.

Retos de la gestión del servicio de TI

La finalidad de ITIL® (23), es proporcionar guías de calidad para la prestación de servicios de TI además de los procesos, funciones y otras competencias necesarias para sustentarlos.

Figura N° 4: Ubicación geográfica ARCOPA S.A



Fuente: Gestión de servicios de TI (23).

Mejores prácticas

ITIL® (24), se define como una biblioteca que documenta las buenas prácticas de Gestión de TI, no es una metodología, no da instrucciones, ni asigna tareas a las personas, no propone una estructura organizacional. Los siguientes son los cuatro principios que ITIL® propone como pilares:

1. Procesos: Para alinear el negocio y la gestión de servicios de TI con enfoque en procesos.
2. Calidad: Basada en los procesos con las medidas y mejoramiento continuo de estos.
3. Cliente: Quien es el beneficiario directo de la mejora de los servicios.
4. Independencia: Para mantener las buenas prácticas independientes de métodos y proveedores.

Seguridad Informática

La seguridad informática en las organizaciones tiene como objetivo proteger las instalaciones físicas frente a los conflictos sociales y laborales, la misma está orientada a salvaguardar las propiedades tanto lógica como física de las organizaciones (25).

Para Gómez V. (26), se puede definir a la seguridad informática como cualquier acción que impida la ejecución de operaciones no autorizadas sobre un sistema informático o red de computadoras. En líneas generales, comprende el conjunto de medidas preventivas, de detección y corrección destinadas a proteger los recursos informáticos de una organización.

La confidencialidad hace alusión a la garantía de que cada mensaje transmitido por las redes de comunicaciones o almacenado en un sistema informático pueda ser leído por su legítimo destinatario, garantizando las medidas de seguridad apropiadas para ese objetivo.

La autenticidad, en cambio, refiere a la identidad del creador de un mensaje o documento es legítima, tanto así como la autenticidad de un equipo al cual uno se conecta dentro de una red para brindar un determinado servicio.

La integridad está relacionada con la garantía de que los contenidos de un documento no hayan sido alterados desde su creación o durante su transmisión en red (26).

La seguridad informática (27), es entendida como un proceso, no un producto terminado a implementar en los sistemas o redes de una organización en tanto que tiene que ser constantemente monitoreado y evaluado permanentemente. Este proceso incluye reducir la posibilidad que se produzcan incidentes de seguridad, facilitar la rápida detección de los incidentes de seguridad, minimizar el impacto en el sistema de información, conseguir la rápida recuperación de los daños experimentados, revisión una computadora.

En cuanto al aspecto más importante, el técnico, incluye el nivel físico (hardware) como el nivel lógico (software) y comprende la ejecución de las medidas de seguridad implementadas por una organización para la protección de los sistemas informáticos y sus redes de comunicación. El proceso de análisis y gestión de riesgos de un sistema informático comprende una etapa de evaluación de los sistemas y redes de una organización y tiene como objetivo la implementación de un plan para la implantación de medidas de seguridad basado en la evaluación de los posibles riesgos y amenazas que pueden afectar a un sistema informático (27).

Las amenazas son eventos accidentales o intencionados que puede ocasionar algún daño al sistema informático y ocasionar pérdidas materiales o financieras o de otro tipo. Existen diferentes tipos de amenazas; naturales (incendios, inundación, tormenta, fallas eléctricas, explosiones, etc.); agentes externos (ataques de una organización criminal, sabotajes, disturbios y conflictos sociales, robos, estafas, virus informáticos, etc.); y agentes internos (descuidos del personal, errores involuntarios en el manejo de herramientas, sabotaje por parte de empleados descontentos, entre otras) (27).

Una vulnerabilidad es una debilidad que presenta un sistema informático que puede permitir que las amenazas causen daños en los mismos y así producir pérdidas para la organización, mientras que un incidente de seguridad es un evento que puede producir una interrupción de los servicios brindados por un sistema informático y/o posibles pérdidas materiales o financieras.

Un plan de seguridad, incluye al conjunto de decisiones que definen las acciones futuras y los medios a utilizar para tal fin, mientras que los procedimientos de seguridad son tareas y operaciones a ejecutar de acuerdo a las políticas de seguridad de la organización (27).

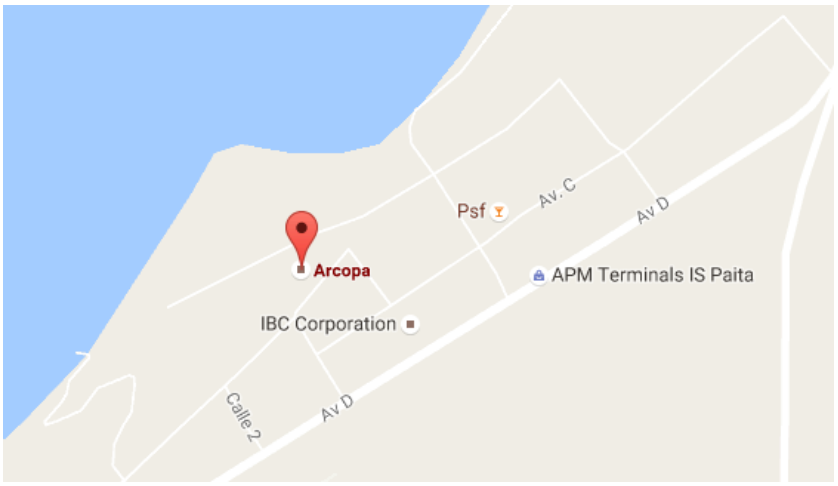
Por último todas las organizaciones realiza auditorías de seguridad periódicas para comprobar la correcta implementación de la política de seguridad que incluye medidas tales como el análisis de posibles vulnerabilidades del sistema informático empleando herramientas de software para localizarlas automáticamente; la revisión de la instalación y configuración de equipos de seguridad tales como antivirus, cortafuegos, etc.; y la realización de pruebas de intrusión, entre otros, logrando identificar por las funciones de prevenir y detectar el mal uso de un sistema informático, abarcando una serie de medidas de seguridad y busca garantizar que todo recurso de un sistema de información sea utilizado tal como una organización o un usuario lo ha decidido, sin intromisiones, implicando el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente (25).

2.3. El rubro de la Empresa

Ubicación Geográfica

La planta industrial se encuentra ubicada en la AV. A Nro. 4041 Zona Industrial (MZ F Lote 1) Piura - Paita - Perú.

Figura N° 5: Ubicación geográfica ARCOPA S.A



Fuente: Google Maps.

Base Legal

- Que por Resolución Directoral N° 020-99-PE/DNPP, del 4 de marzo de 1999, se otorgó a la Empresa ARMADORES Y CONGELADORES DEL PACIFICO S.A. – ARCOPA S.A. licencia de operación, para que desarrolle la actividad de procesamiento de recursos hidrobiológicos, destinado al consumo humano directo, a través de su planta de congelado, con una capacidad de 50 t/día, en su establecimiento industrial pesquero ubicado en la Zona Industrial II de Paita, Mz. F, Lote 1, distrito y provincia de Paita, departamento de Piura

- En uso de las facultades conferidas por el artículo 118° del Reglamento de la Ley General de Pesca, aprobado por Decreto Supremo Nº 012-2001-PE; se resuelve:

  Artículo 1°.- Otorgar a la Empresa ARMADORES Y CONGELADORES DEL PACÍFICO S.A. – ARCOPA S.A. autorización para efectuar el incremento de la capacidad instalada de la planta de congelado de productos hidrobiológicos, e instalar una

planta de harina de pescado residual, accesoria y complementaria al funcionamiento de la citada actividad, y ser de uso exclusivo para el procesamiento de los residuos y pescado descartado provenientes de su planta de congelado, en su establecimiento industrial pesquero, ubicado en Av. A Nº 4041, Mz F1, Zona Industrial II, distrito y provincia de Paita, departamento de Piura, con las siguientes capacidades proyectadas:

Congelado: de 50 a 125 t/día

Harina de pescado residual: 10 t/h

Áreas de la Empresa

- Área Gerencial

  Responsable de liderar y coordinar las funciones del planeamiento estratégico de la Empresa, teniendo en cuenta todas las funciones de mercadeo, ventas, finanzas y de recursos humanos de la Empresa, así como también de las operaciones del día a día.

- Área Producción.- Teniendo como función principal, la transformación de insumos o recursos (energía, materia prima, mano de obra, capital, información) en productos finales (bienes o servicios).

- Área de Importación y Exportación.- Encargados de la base del comercio internacional, requiriendo la participación de las aduanas, tanto en el país de importación como en el país de exportación y son a menudo sujetos a cuotas de importación, aranceles y acuerdos comerciales, ya que es de mucha importante para el crecimiento y desarrollo sostenido a largo plazo de la Empresa.

- Área RR.HH.- La función primordial que cumplen es seleccionar, contratar, formar, emplear y retener a los colaboradores de la Empresa, cuidar el capital humano, ayudar a que la Empresa desarrolle su actividad con el nivel de conflicto lo más bajo posible.

- Área Contabilidad.- Responsables de determinar el balance global de su riqueza, beneficio, liquidez, los presupuestos de las actividades de marketing, la reinversión de utilidades, el desarrollo e investigación, y el crecimiento de la compañía, todo depende del trabajo de los contables.

- Área Logística.- Responsables de cubrir la gestión y la planificación de actividades de los departamentos de compras, producción, transporte, almacenaje, manutención y distribución, satisfaciendo la demanda en las mejores condiciones de servicio, costo y calidad de la Empresa.

- Área Mantenimiento.- Encargados de proporcionar oportuna y eficientemente, los servicios que requiera el centro en materia de mantenimiento preventivo y correctivo a las instalaciones, así como la contratación de la obra pública necesaria para el fortalecimiento y desarrollo de las instalaciones físicas de los inmuebles.

- Área Seguridad Industrial.- Esta área multidisciplinaria está encargada de minimizar los riesgos en la industria, ya que gracias a ella es una parte esencial para una Empresa que trae consigo muchos beneficios al evitar grandes pérdidas utilizando una estrategia de seguridad e implementación.

- Área Sistemas.- Área encargada del diseño, implementación y mantenimiento de los elementos que constituyen lo que podemos llamar la infraestructura informática de la Empresa, proporcionando a

toda la comunidad los servicios informáticos necesarios para desarrollar sus actividades.

- Área Taller.- Es aquella área dedicada a la reparación del equipamiento y maquinaria de la Empresa, brindando respaldo a sus productos.

Reseña Histórica

Armadores y Congeladores del Pacífico S.A; ARCOPA, es una de la principales Empresas peruanas de procesamiento de congelación del pescado con destino al consumo humano, entrando así en el marco de la política peruana para la diversificación del sector pesquero, fundada en 1993 con el fin de especializarse en la pesca y transformación de productos del mar; llegando a enfocarse en la búsqueda del desarrollo económico de la pesca en el Perú; logrando ser, una de las principales Empresas peruanas en el procesamiento y congelamiento del recurso hidrobiológico destinado al consumo humano.

Especializada desde su origen en la pesca de merluza, ARCOPA se ha diversificado hacia el procesamiento de otras especies como Pota o Calamar Gigante, Calamar, Conchas de Abanico, Mahi Mahi o Perico, Anchoveta entre las principales especies, ofreciendo a sus clientes una amplia gama de productos de consumo humano.

En la búsqueda del aprovechamiento de los recursos hidrobiológicos de nuestro mar, ARCOPA, ha desarrollado un técnica en la producción de surimi-base a partir de las diferentes especies que procesamos, siendo el primer productor de surimi-base de anchoveta en el mundo.

La planta está ubicada en Paita, noroeste del Perú; con una extensión de más de 40,000 m2, una capacidad de recepción de materia prima de 200 toneladas/día y congelación de producto terminado de 125 toneladas/día. Las herramientas de producción en el área de procesamiento son:

• 7 líneas de fileteo.
• 3 líneas de fabricación de surimi - base de pescado.
• 1 línea de fabricación de surimi - base de pota.
• 1 línea de cocción.

Asimismo, cuenta con una flota propia de pesca, integrada por 8 embarcaciones de arrastre para la pesca de Merluza, y a través de la pesca artesanal local se abastece de las demás especies que se procesan.

Cuenta también con una línea de producción de harina y aceite de pescado Residual de 10 TN / Hora proveniente de los subproductos generados por el proceso de congelados.

ARCOPA está enfocada al desarrollo de productos nuevos de acuerdo a los requerimientos del cliente/mercado, cumpliendo con los estándares internacionales de calidad que se necesitan

Visión

Nuestra visión es ser una empresa de clase mundial a la vanguardia, líder e innovadora en el aprovechamiento sostenible de recursos hidrobiológicos de origen marinos de un alto valor agregado para el consumo humano, logrando contribuir al progreso de la industria pesquera.

Misión

Nuestra misión es aprovechar la posición estratégica del puerto de Paita como un punto importante en la conexión intermodal Atlántico-Pacifico y convertirlo en un puerto hub regional con altos estándares de calidad, eficiencia y seguridad en beneficio del comercio internacional (28).

Figura N° 6: Frontal de Empresa ARCOPA S.A

Fuente: Elaboración propia

Objetivos organizacionales

a) Establecer objetivos que sirven como una guía para la etapa de ejecución de las acciones.
b) Justificar actividades que realizan cada una de las áreas.
c) Evaluar las acciones y la eficacia de la organización.
d) Verificar la eficiencia y comparar la productividad de la organización.
e) Revisar continuamente la estructura de los objetivos frente a las alteraciones del medio ambiente y de la organización (28).

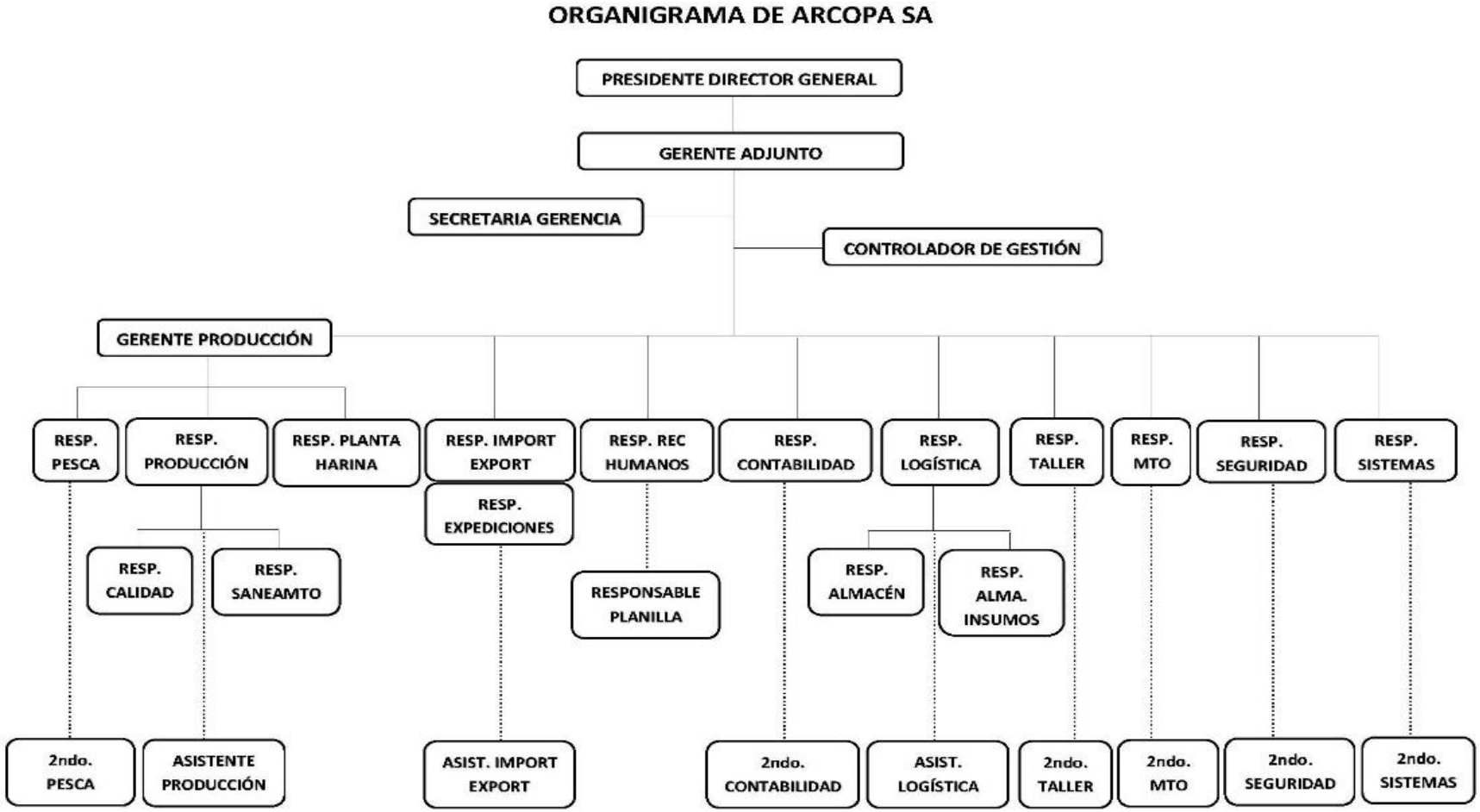
Funciones

a) Diseñar y ejecutar programas dirigidos a la diversificación de ayudas económicas para la mejora de la competitividad de las Empresas pesqueras.
b) Proponer la articulación de subvenciones y elaborar y ejecutar programas y actuaciones en todos sus ámbitos de intervención.
c) Ordenar, gestionar y promover la explotación de los recursos marítimo-pesqueros y de la pesca continental.
d) Promover y aprobar proyectos de carácter experimental en materia de pesca (28).

e) Ordenar y gestionar la pesca deportiva y expedición de las correspondientes licencias.
f) Asistir y apoyar a la flota pesquera en situaciones especiales que lo hagan preciso.
g) Gestionar y promover las medidas correspondientes en relación con los instrumentos y garantías establecidos para el sector pesquero.
h) Planificar y dirigir el Servicio de Inspección Pesquera, realizando las actuaciones necesarias para garantizar un funcionamiento eficaz del mismo (28).

Organigrama:

Figura N° 7: Organigrama de la Empresa ARCOPA S.A



Fuente: Elaboración propia**,** recopilación de datos de la Empresa ARCOPA S.A

Infraestructura tecnológica existente

Hardware

Tabla N° 1: Equipos Tecnológicos de la Empresa ARCOPA S.A

Recursos	Software – marcas	N°
Computadoras	Compaq, Samsung	38
	Laptops	2
Impresoras	Epson l220/ Epson fx-890/ HP Laserject	8
	Scanner HP Scanket 2410	2
Dispositivos	Access Point	2
	Router	1
	Switch	9
Servidores	1. Servidor de bases de datos Oracle - HP PROLIANT ML 310 2. Servidor de dominio de respaldo - HEWLETT PACKARD ENTERPRISE 3. De dominio, Windows Server 2018 R2. 4. Servidor de Correos. 5. Servidor de Sistema ERP SIGRE. 6. Servidor Web. 7. Firewall.	7

Fuente: Elaboración propia, recopilación de datos de la Empresa ARCOPA S.A

Software

Tabla N° 2: Software adquiridos en la Empresa ARCOPA S.A

Software	Descripción
Sistemas Operativos	Windows Server 2008 Windows XP, Windows 7, Windows 8, Windows 10
Ofimática	Office 2007, 2013,2016 Adobe Acrobat
Navegador Web	Internet Explorer, Mozilla Firefox, Chrome Google
Antivirus	Eset Endpoint Antivirus V.6

Fuente: Elaboración propia, recopilación de datos de la Empresa ARCOPA S.A

Aplicaciones

Tabla N° 3: Aplicaciones que maneja la Empresa ARCOPA S.A

Aplicaciones	Funcionalidad
Zimbra	Servidor de correos corporativos que maneja la Empresa.
SIGRE	Es un sistema informático ERP que permite administrar, supervisar y manejar las operaciones de las entradas, salidas, reportes y gastos de la Empresa.

Fuente: Elaboración propia, recopilación de datos de la Empresa ARCOPA S.A

2.4. Las tecnologías de la información y comunicaciones

Definición

Cabero (29), en el año 1998, "En líneas generales podríamos decir que las nuevas tecnologías de la información y comunicación son las que giran en torno a tres medios básicos: la informática, la microelectrónica y las telecomunicaciones; pero giran, no sólo de forma aislada, sino lo que es más significativo de manera interactiva e interconexionadas, lo que permite conseguir nuevas realidades comunicativas".

Las características que diferentes autores especifican como representativas de las TIC, recogidas por Cabero (29), son:

- **Inmaterialidad** En líneas generales podemos decir que las TIC realizan la creación, el proceso y la comunicación de la información. Esta información es básicamente inmaterial y puede ser llevada de forma transparente e instantánea a lugares lejanos.
- **Interactividad**. La interactividad es posiblemente la característica más importante de las TIC para su aplicación en el campo educativo, logrando conseguir un intercambio de información entre el usuario y el ordenador.
- **Interconexión**. La interconexión hace referencia a la creación de nuevas posibilidades tecnológicas a partir de la conexión entre dos tecnologías.
- **Instantaneidad**. Las redes de comunicación y su integración con la informática, han posibilitado el uso de servicios que permiten la comunicación y transmisión de la información, entre lugares alejados físicamente, de una forma rápida.
- **Digitalización**. Su objetivo es que la información de distinto tipo (sonidos, texto, imágenes, animaciones, etc.) pueda ser transmitida por los mismos medios al estar representada en un formato único universal.

Según Marqués G. (30), en su investigación específica, que al unir estas tres palabras hacemos referencia al conjunto de avances tecnológicos que nos

proporcionan la informática, las telecomunicaciones y las tecnologías audiovisuales, que comprenden los desarrollos relacionados con los ordenadores, Internet, la telefonía, las aplicaciones multimedia y la realidad virtual, estas tecnologías básicamente nos proporcionan información, herramientas para su proceso y canales de comunicación.

"Las tecnologías de la información y de las comunicaciones (TIC) son términos que se utilizan actualmente para hacer referencia a una gama amplia de servicios, aplicaciones y tecnologías, que utilizan diversos tipos de equipos y de programas informáticos, y que a menudo se transmiten a través de las redes de telecomunicaciones" (31).

Parafraseando la definición de González E. (32), entendemos por "nuevas tecnologías de la Información y la Comunicación" el conjunto de procesos y productos derivados de las nuevas herramientas (hardware y software), soportes de la información y canales de comunicación relacionados con el almacenamiento, procesamiento y transmisión digitalizados de la información.

Cabero J. (33), en su trabajo de Investigación, ha sintetizado las características más distintivas de las nuevas tecnologías en los siguientes rasgos: inmaterialidad, interactividad, instantaneidad, innovación, elevados parámetros de calidad de imagen y sonido, digitalización, influencia más sobre los procesos que sobre los productos, automatización, interconexión y diversidad."

Canseco F. (34), hace mención que: "Tecnología es la propiedad para aplicar los conocimientos de la Ciencia en los procesos de producción. La Tecnología sería así el lazo de unión de las ideas científicas y la aplicación práctica de dichas ideas".

Como lo menciona Salazar O. (35), las TIC, cubren las necesidades de comunicación y de procesamiento de la información en una organización, es decir, que permiten la adquisición, el almacenamiento, la manipulación y la

distribución o transmisión de la información, para lo cual se valen de dispositivos, herramientas, equipos, componentes electrónicos y redes de interconexión.

Objetivo de las TIC

Las tecnologías de la información y la comunicación (TIC, TICs o bien NTIC para Nuevas Tecnologías de la Información y de la Comunicación o IT para «Information Technology») agrupan los elementos y las técnicas utilizadas en el tratamiento y la transmisión de las informaciones, principalmente de informática, internet y telecomunicaciones (36).

Por Tecnologías de la información o tecnologías de la información y de la comunicación (TIC) se entiende un término dilatado empleado para designar lo relativo a la informática conectada a Internet, y especialmente el aspecto social de éstos. Ya que las nuevas tecnologías de la información y comunicación designan a la vez un conjunto de innovaciones tecnológicas pero también las herramientas que permiten una redefinición radical del funcionamiento de la sociedad; Un buen ejemplo de la influencia de los TIC sobre la sociedad es el gobierno electrónico (36).

En resumen las nuevas tecnologías de la información y comunicación son aquellas herramientas computacionales e informáticas que procesan, almacenan, sintetizan, recuperan y presentan información representada de la más variada forma. Es un conjunto de herramientas, soportes y canales para el tratamiento y acceso a la información. Constituyen nuevos soportes y canales para dar forma, registrar, almacenar y difundir contenidos informacionales. Algunos ejemplos de estas tecnologías son la pizarra digital (ordenador personal + proyector multimedia), los blogs, el podcast y, por supuesto, la web (36).

Para todo tipo de aplicaciones educativas, las TIC son medios y no fines. Es decir, son herramientas y materiales de construcción que facilitan el aprendizaje,

el desarrollo de habilidades y distintas formas de aprender, estilos y ritmos de los aprendices (36).

Si elaborásemos una lista con los usos que hacemos de las Tecnologías de la Información y la Comunicación sería prácticamente interminable:

- Internet de banda ancha
- Teléfonos móviles de última generación.
- Televisión de alta definición.

Las Tecnologías de la información y la comunicación están presentes en nuestras vidas y la han transformado.

La tecnología digital, unida a la aparición de ordenadores cada vez más potentes, ha permitido a la humanidad progresar muy rápidamente en la ciencia y la técnica desplegando un arma muy poderosa como: la información y el conocimiento. Pero no sólo eso, las tecnologías de la información y la comunicación han transformado la gestión de las Empresas y nuestra la manera de hacer negocios (36):

- Para comunicarnos con nuestros clientes.
- Para gestionar pedidos.
- Para promocionar nuestros productos.
- Para relacionarnos con la administración pública.

En todas las áreas de la gestión Empresarial, las TIC han transformado nuestra manera de trabajar, liberándonos de las cargas más pesadas, optimizando nuestros recursos y haciéndonos más productivos, ya que gracias a ellas, somos capaces de producir mucho más, de mejor calidad (36).

Ventajas de la TIC

En entorno Márquez J. (37), muestra las relaciones existentes, las nuevas tecnologías y las posibilidades que las Empresas u organizaciones tienen al acceder, conocerlas y utilizarlas, inciden en la apropiación de las innovaciones tecnológicas por las mismas, ya que se tiene en cuenta que los procesos de innovación tecnológica pueden ser entendidos como un proceso de innovación social que moviliza las capacidades de la organización, las ventajas son:

- Impartir nuevos conocimientos para la empleabilidad que requieren muchas competencias (integración, trabajo en equipo, motivación, disciplina, etc.).

- Ofrecer nuevas formas de trabajo.

- Dar acceso al flujo de conocimientos e información para empoderar y mejorar las vidas de las personas, mantiene menores riesgos y menores costos.

Desventajas de las TIC

Márquez J. (37), recalca las desventajas que se pueden observar en la utilización de las tecnologías de información y comunicación son las siguientes:

- Falta de privacidad.
- Aislamiento.
- Fraude.
- Merma los puestos de trabajo.

Características de las TIC

Las Tecnologías de Información y Comunicación tienen características muy importantes y principales (37):

- Son de carácter innovador y creativo, pues dan acceso a nuevas formas de comunicación, teniendo mayor influencia y beneficia en mayor proporción al área educativa ya que la hace más accesible y dinámica.

- Son considerados temas de debate público y político, pues su utilización implica un futuro prometedor.

- Se relacionan con mayor frecuencia con el uso del internet y la informática.

- Afectan a numerosos ámbitos de la ciencia humana como la sociología.

Impacto de las TIC en las Empresas u organizaciones

Las Empresas u organizaciones están abiertas a los impactos de los sistemas de información como lo menciona Restrepo L. (38), que estos deben estar alineados con los objetivos de la organización. Existen unos factores mediadores que influyen en la interacción entre las TIC y las organizaciones.

Hay varios tipos de definiciones: desde las definiciones centradas en el aspecto técnico que consideran la organización como un conjunto de recursos procesadores para producir una salida en forma de productos o servicios, hasta las definiciones centradas en los comportamientos, que hablan de un conjunto de derechos, responsabilidades y obligaciones (38).

Al implantar nuevas tecnologías de informática y comunicaciones, los patrones de trabajo y las habilidades que ellos requieren, podrán ser muy diferentes de los que se tenían antes. También estas tecnologías ofrecen la posibilidad de desarrollar trabajos en la sede del cliente, o en la residencia del trabajador (teletrabajo), manteniendo en todo momento la necesaria comunicación e intercambio de información con la sede de la organización (38).

Importancia de la Auditoría enfocada a las TIC

Aranguiz G; Cabello N; Riquelme E; Rivas K; Rodríguez J; Silva R. (39), enfocan la importancia, ya que hace referencia al conjunto de avances tecnológicos que nos proporciona la informática, las telecomunicaciones y las tecnologías audiovisuales, que comprenden los desarrollos relacionados con los ordenadores, internet, la telefonía, las aplicaciones multimedia y la realidad virtual, estas tecnologías nos proporcionan información, herramientas para su proceso y canales de comunicación.

Las distintas áreas operativas de las organizaciones se sostienen y apoyan cada vez más en los servicios de las TIC, ya que han acompañado la automatización y el crecimiento de todos los procesos productivos y la prestación de nuevos servicios, representando los activos más valiosos, y a su vez, reconocen los beneficios potenciales de las nuevas tecnologías (39).

2.5. Seguridad de las Tecnologías de Información y Comunicación

Para llegar a introducirnos en el tema de la Seguridad de las TIC, Romero L. (40), califica que es necesario tener en cuenta los conceptos principales de STIC, para ello hemos tomado en cuenta lo siguiente:

Seguridad.- Se refiere a la ausencia de riesgos, encargada de estudiar, evaluar y gestionar los riesgos, el termino se puede tomar diversos sentidos según al campo que haga referencia (40).

Tecnologías.- Es la aplicación de los conocimientos científicos para facilitar la realización de las actividades humanas; enfocada en el estudio, investigación, desarrollo e innovación de los procedimientos y técnicas empleados en la transformación de la información (40).

Información.- Es el conjunto de datos, que permite a los individuos o sistemas qué poseen dicho conocimientos para la toma de decisiones. De la cual en ella vamos a tomar decisiones que dan lugar a todas nuestras acciones (40).

Comunicación.- Es aquella transmisión de mensajes entre un conjunto de personas, ya que además de recibir la información, necesitamos comunicarnos y expresar nuestras opiniones, como un sistema de apoyo y bienestar para la sociedad u organización (40).

En los últimos tiempos los sistemas informáticos se han introducido de forma generalizada en el comercio, banca, industria, administración, defensa, investigación, la aparición y expansión de Internet, juntamente con los sistemas informáticos, han hecho posible la realización de un sin número de tareas y a medida que los sistemas de información son más complejos, han puesto de manifiesto una mayor cantidad de puntos vulnerables (40):

1. El número de posibles atacantes crece muy rápidamente.

2. Los medios disponibles para efectuar ataques siguen una evolución tan rápida como los propios sistemas.

3. La generalización de Internet hace que los ataques puedan provenir de cualquier lugar.

El concepto de seguridad de las TIC es mucho más amplio que la simple protección de los datos desde un punto de vista lógico, interviniendo factores tecnológicos pero también aspectos como la protección física, las salvaguardas organizativas o el cumplimiento normativo y teniendo en cuenta múltiples condicionantes, tanto internos como externos a una Organización (41).

Así, la Seguridad de las Tecnologías de la Información y Comunicaciones hace referencia al conjunto de medidas de seguridad para proteger la información

almacenada, procesada o transmitida por sistemas de información y telecomunicaciones, de manera que se preserve la confidencialidad, integridad y disponibilidad de la información y la integridad y la disponibilidad de los elementos que la tratan (41).

2.6. Marcos de referencia

ITIL (Biblioteca de Infraestructura de Tecnologías de Información)

Según Nacipucha E. (42), en el año 2011, describe en su tesis que Information Technology Infraestructure Library (ITIL), es una metodología que se basa en la calidad de servicio y el desarrollo eficaz y eficiente de los procesos que cubren las actividades más importantes de las organizaciones en sus Sistemas y Tecnologías de Información, la cual esta metodología fue desarrollada a petición del Gobierno del Reino Unido a finales de los 80 y recoge las mejores prácticas en la gestión de los Sistemas de Información. Desde entonces se ha ido extendiendo su uso en toda la Empresa privada, tanto multinacional como PYME, llegando a ser considerado un estándar de facto para la gestión de esta área de la Empresa.

García C. (43), define a ITIL como metodología propone el establecimiento de estándares que nos ayuden en el control, operación y administración de los recursos (ya sean propios o de los clientes). Plantea hacer una revisión y reestructuración de los procesos existentes en caso de que estos lo necesiten (si el nivel deficiencia es bajo o que haya una forma más eficiente de hacer las cosas), lo que nos lleva a una mejora continua, mediante la cual esta metodología fue desarrollada a finales de los años 80’s por iniciativa del gobierno del Reino Unido, específicamente por la OGC u Oficina Gubernativa de Comercio Británica (Office of Goverment Comerce).

Según Seguinfo (44), ITIL es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI) de alta calidad. ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir de guía para que abarque toda infraestructura, desarrollo y operaciones de TI.

Aunque se desarrolló durante los años 1980, ITIL no fue ampliamente adoptada hasta mediados de los años 1990. ITIL se considera a menudo junto con otros marcos de trabajo de mejores prácticas como la Information Services Procurement Library (ISPL, 'Biblioteca de adquisición de servicios de información'), la Application Services Library (ASL, 'Biblioteca de servicios de aplicativos'), el método de desarrollo de sistemas dinámicos (DSDM, Dynamic Systems Development Method), el Modelo de Capacidad y Madurez (CMM/CMMI) y a menudo se relaciona con la gobernanza de tecnologías de la información mediante COBIT (Control Objectives for Information and related Technology), (44).

Objetivos de ITIL

Según estos autores Cervantes D; Rivera L; Vallecillo J. (45), menciona los siguientes objetivos:

- Alinear los servicios de TI con las necesidades de la Empresa(negocio), actuales y futuras
- Mejorar la calidad de los servicios de TI.
- Reducir los costos por la proveeduría de servicios de TI en el mediano largo plazo.

Ventajas de ITIL

- Mejora la comunicación con los clientes y usuarios finales a través de los diversos puntos de contacto acordados.
- Los servicios se detallan en lenguaje del cliente y con más detales, manejando mejor la calidad y los costos de los servicios.
- La entrega de servicios IT se enfoca más al cliente, mejorando con ello la calidad de los mismos.
- La organización TI desarrolla una estructura más clara, se vuelve más eficaz, y se centra más en los objetivos de la organización.
- La administración tiene un mayor control, se estandarizan e identifican los procedimientos, y los cambios resultan más fáciles de manejar.
- A través de las mejores prácticas de ITIL se apoya al cambio en la cultura de TI y su orientación hacia el servicio, proporcionando un marco de referencia uniforme para la comunicación interna y con proveedores (45).

Desventajas de ITIL

- Tiempo y esfuerzo necesario para su implementación
- Que no se vea reflejada una mejora por falta de entendimiento, sobre procesos, indicadores y como pueden ser controlados.
- Que el personal no se involucre y se comprometa.
- La mejora del servicio y la reducción de costos puede no ser visible.
- Que la inversión en herramientas de soporte sea escasa los procesos podrán parecer inútiles y no se alcancen las mejoras en los servicios (45).

COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas)

Es una herramienta para la administración de las tecnologías de información. Fue desarrollada por ISACA (46), está orientado a la gestión, auditoría de sistemas, control y seguridad. Define lo que es necesario hacer para implementar una efectiva estructura de control. La gestión y administración de una organización debe garantizar que exista una plataforma de control interno que dé soporte a los procesos de negocio. COBIT se concentra en los requerimientos del negocio relacionados a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información que fluye en la organización.

COBIT (47), fue publicado por primera vez por ITGI en abril de 1996. Su última actualización – COBIT® 4.1 hace énfasis en el cumplimiento reglamentario, ayudando a la organizaciones a incrementar el valor de TI, destacando los vínculos entre los objetivos del negocio y TI, y simplificando la implementación del marco de trabajo COBIT. Este marco de trabajo es la base para diferentes entes reguladores a nivel mundial, con la finalidad de lograr que las entidades reguladas optimicen sus inversiones de TI y administren adecuadamente sus riesgos tecnológicos.

Según Osorio L. (48), COBIT es un marco de trabajo y un conjunto de herramientas de Gobierno de Tecnología de Información (TI) que permite a la Gerencia cerrar la brecha entre los requerimientos de control, aspectos técnicos y riesgos de negocios. COBIT habilita el desarrollo de políticas claras y buenas prácticas para el control de TI a lo largo de las organizaciones.

Según Marin B. (49), COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva de negocios.

Según señaló un informe de ETEK (50), "La adecuada implementación de un modelo COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado".

Según Puig J. y Blanco S. (51), el estándar COBIT ofrece un conjunto de "mejores prácticas" para la gestión de los Sistemas de Información de las organizaciones. El objetivo principal de COBIT consiste en proporcionar una guía a alto nivel sobre puntos en los que establecer controles internos con tal de:

- Asegurar el buen gobierno, protegiendo los intereses de los clientes.
- Garantizar el cumplimiento normativo del sector al que pertenezca la organización.
- Mejorar la eficiencia de los procesos y actividades de la organización.
- Garantizar la confidencialidad, integridad y disponibilidad de la información.

Criterios de información de COBIT

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio, para ello se definieron los siguientes siete criterios de información (52):

La efectividad.- tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.

La eficiencia.- consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.

La confidencialidad.- se refiere a la protección de información sensitiva contra revelación no autorizada.

La integridad.- está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.

La disponibilidad.- se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.

El cumplimiento.- tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.

La confiabilidad.- se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno (52).

Marco de trabajo de COBIT

COBIT (53), se basa en el análisis y armonización de estándares y mejores prácticas de TI existentes y se adapta a principios de gobierno

generalmente aceptados. Está posicionado a un nivel alto, impulsado por los requerimientos del negocio, cubre el rango completo de actividades de TI, y se concentra en lo que se debe lograr en lugar de como lograr un gobierno, administración y control efectivos. Está diseñado para ser complementario y para ser usado junto con otros estándares y mejores prácticas.

La implantación de las mejores prácticas debe ser consistente con el gobierno y el marco de control de la Empresa, debe ser apropiada para la organización, y debe estar integrada con otros métodos y prácticas que se utilicen. Son más útiles cuando se aplican como un conjunto de principios y como un punto de partida para adaptar procedimientos específicos. La gerencia y el equipo deben entender qué hacer, cómo hacerlo y porqué es importante hacerlo (53).

COBIT resulta de interés a distintos usuarios (53):

- Dirección ejecutiva.- Para obtener valor de las inversiones y para balancear las inversiones en riesgo y control en un ambiente de TI con frecuencia impredecible

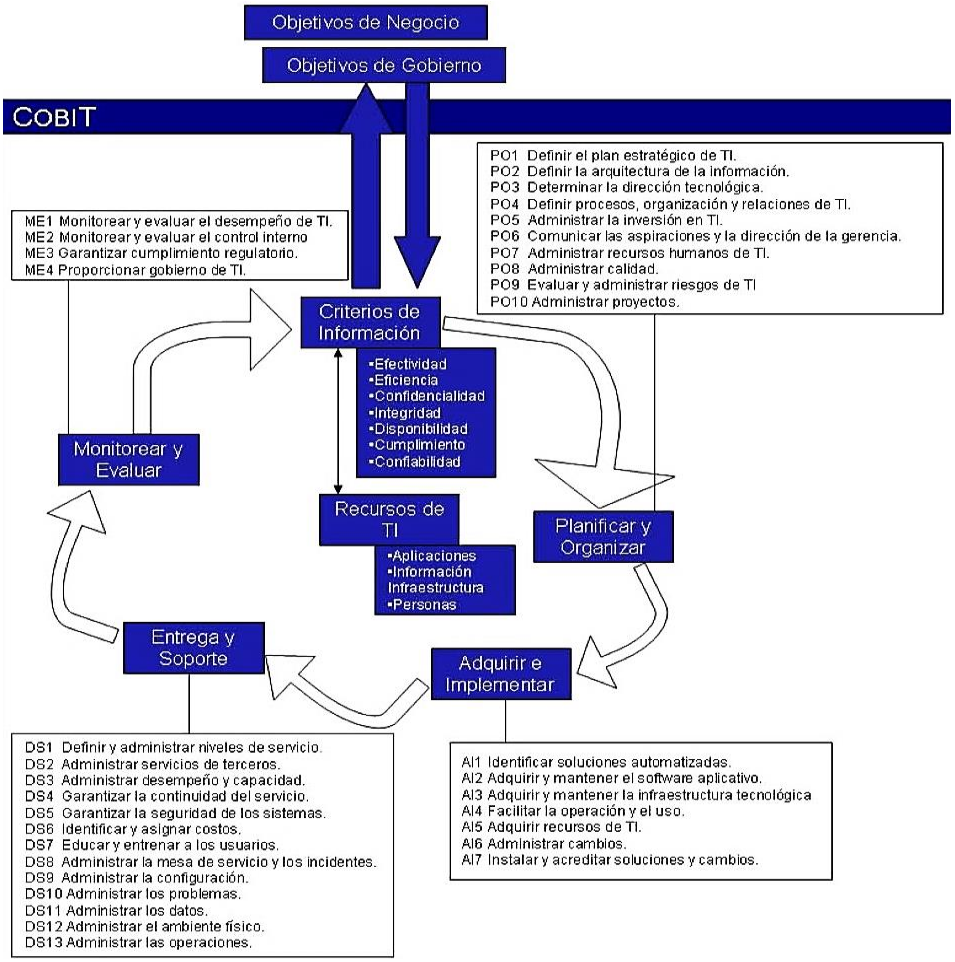
- Gerencia del negocio.- Para obtener certidumbre sobre la administración y control de los servicios de TI, proporcionados internamente o por terceros.

- Gerencia de TI.- Para proporcionar los servicios de TI que el negocio requiere para dar soporte a la estrategia del negocio de una forma controlada y administrada.

- Auditores.- Para respaldar sus opiniones y/o para proporcionar asesoría a la gerencia sobre controles internos.

COBIT (53), ha sido desarrollado y mantenido por un instituto de investigación sin ánimo de lucro, basándose en una investigación continua sobre las mejores prácticas de TI y se le da un mantenimiento continuo, proporcionando así un recurso objetivo y práctico para todo tipo de usuario.

Figura N° 8: Marco de trabajo de COBIT



Fuente: Rolling Meadows (53).

Recursos de TIC identificados en COBIT (54)**:**

Las aplicaciones incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información. La

información son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información.
ISACA (46), hace mención que la infraestructura es la tecnología y las instalaciones que permiten el procesamiento de las aplicaciones. Las personas son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. COBIT define las actividades de TI en un modelo de 34 procesos genéricos agrupados en 4 dominios:

Planear y Organizar (PO).- Estrategias y tácticas. Identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio (46).

Adquirir e Implementar (AI).- Identificación de soluciones, desarrollo o adquisición y mantenimiento de sistemas existentes. Proporciona las soluciones y las pasa para convertirlas en servicios (46).

Entregar y Dar Soporte (DS).- Cubre la entrega de los servicios requeridos. Incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales (46).

Monitorear y Evaluar (ME).- Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño del control interno, el cumplimiento regulatorio y la aplicación del gobierno (46).

Procesos:

Planear y organizar (po)

- PO1 Definir el plan estratégico de TI.

- PO2 Definir la arquitectura de la información
- PO3 Determinar la dirección tecnológica.
- PO4 Definir procesos, organización y relaciones de TI.
- PO5 Administrar la inversión en TI.
- PO6 Comunicar las aspiraciones y la dirección de la gerencia.
- PO7 Administrar recursos humanos de TI (52).

Adquirir e implementar (ai)

- AI1 Identificar soluciones automatizadas.
- AI2 Adquirir y mantener el software aplicativo.
- AI3 Adquirir y mantener la infraestructura tecnológica
- AI4 Facilitar la operación y el uso.
- AI5 Adquirir recursos de TI.
- AI6 Administrar cambios.
- AI7 Instalar y acreditar soluciones y cambios (52).

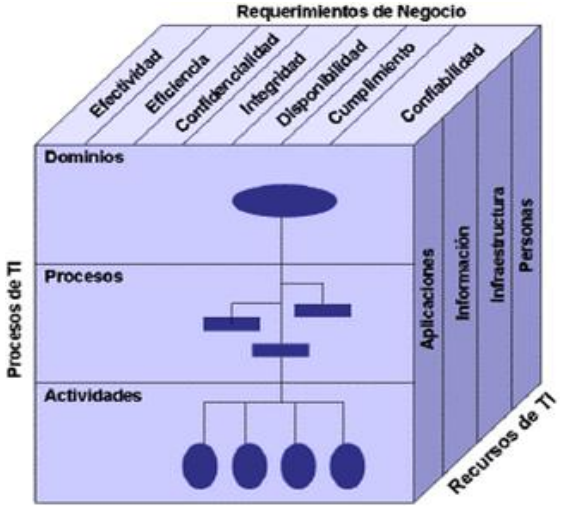
Entregar y dar soporte (ds)

- DS1 Definir y administrar niveles de servicio.
- DS2 Administrar servicios de terceros.
- DS3 Administrar desempeño y capacidad.
- DS4 Garantizar la continuidad del servicio.
- DS5 Garantizar la seguridad de los sistemas.
- DS6 Identificar y asignar costos.
- DS7 Educar y entrenar a los usuarios.
- DS8 Administrar la configuración.
- DS9 Administrar los problemas.
- DS10 Administrar los datos.
- DS11 Administrar el ambiente físico.
- DS12 Administrar las operaciones (52).

Monitorear y evaluar (me)

- ME1 Monitorear y evaluar el desempeño de TI.
- ME2 Monitorear y evaluar el control interno
- ME3 Garantizar cumplimiento regulatorio.
- ME4 Proporcionar gobierno de TI (52).

Figura N° 9: Cubo de COBIT



Fuente: ISACA (52).

Importancia de la Medición

Una necesidad básica de toda Empresa es entender el estado de sus propios sistemas de TI y decidir qué nivel de administración y control debe proporcionar. Para decidir el nivel correcto, la gerencia debe preguntarse: ¿Hasta dónde debemos ir?, y ¿está el costo justificado por el beneficio? (52).

La obtención de una visión objetiva del nivel de desempeño propio de una Empresa no es sencilla. ¿Qué se debe medir y cómo? Las Empresas deben medir dónde se encuentran y dónde se requieren mejoras, e

implementar un juego de herramientas gerenciales para monitorear esta mejora. COBIT atiende estos temas a través de (52):

- Modelos de madurez**;** facilitan la evaluación por medio de benchmarking y la identificación de las mejoras necesarias en la capacidad.

- Metas y mediciones de desempeño para los procesos de TI; demuestran cómo los procesos satisfacen las necesidades del negocio y de TI.

Modelo Genérico de Madurez (46)

0. No existente. Carencia completa de cualquier proceso reconocible.

1. Inicial. Existe evidencia que la Empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso.

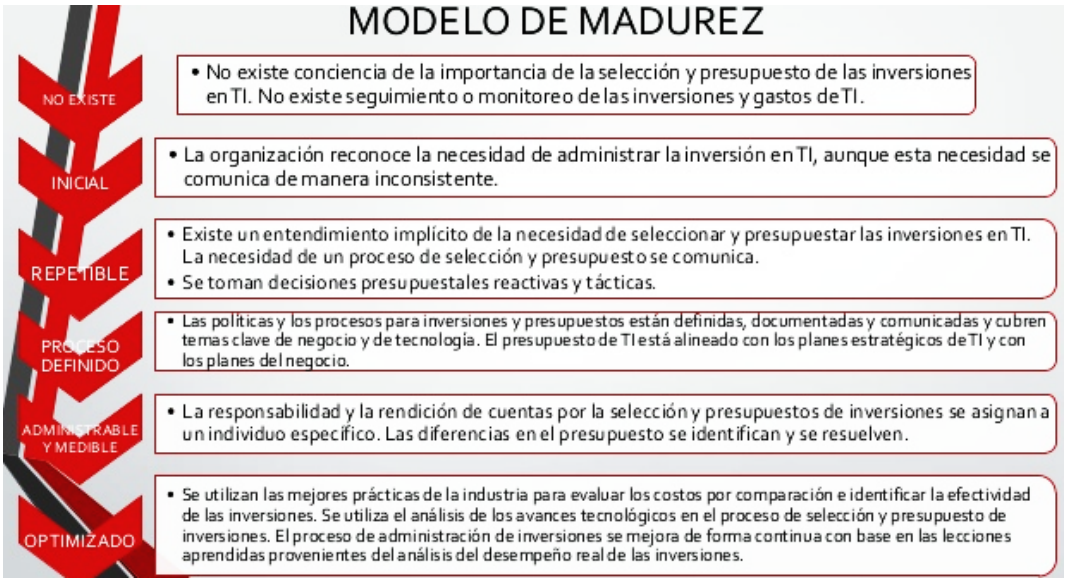
2. Repetible. Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. Existe un alto grado de confianza en el conocimiento de los individuos, no hay entrenamiento.

3. Definido. Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones (46).

4. Administrado. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva.

5. Optimizado. Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras Empresas.

Figura N° 10: Modelos de madurez



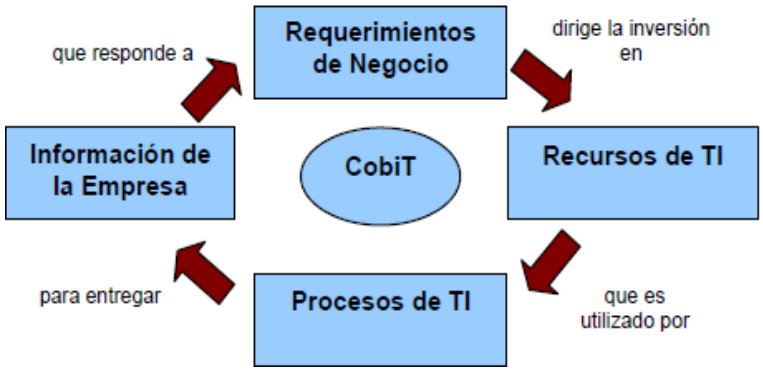
Fuente: Representación gráfica de los modelos de madurez (52).

Principios de COBIT

COBIT maneja el control desde el punto de vista de políticas, estructuras organizacionales y procedimientos. En cuanto a la administración y gestión, son manejadas desde la perspectiva del gobierno corporativo, es decir, señalando los lineamientos para que todos los individuos involucrados en la administración, uso, diseño, desarrollo y mantenimiento de los sistemas de información cumplan con los objetivos del negocio (46).

COBIT es muy importante ya que permite mejorar todas las técnicas para la seguridad, calidad, eficacia, eficiencia, confidencialidad, integridad y disponibilidad de las TIC, permitiendo identificar riesgos, gestionar los recursos y ayuda a medir el desempeño en la organización, para llegar a cumplir las metas propuestas y evaluar el nivel de madurez de las funciones, seguridad y procesos de la organización (46).

Figura N° 11: Principio básico de COBIT



Fuente: Rolling Meadows (53).

Características ITIL vs COBIT

Según Guanajuato L. (55), ITIL es el estándar más ampliamente conocido para la gestión de los servicios TI, ya que una correcta gestión de servicios permite un alto nivel de disponibilidad de dichos servicios y un alto nivel de satisfacción de clientes y empleados de la compañía.

ITIL se centra en brindar servicios de alta calidad para lograr la máxima satisfacción del cliente a un costo manejable. Parte de un enfoque estratégico basado en el triángulo de procesos, personas y tecnología, la cual determina la forma de ejecutar procesos en las tecnologías para lograr la satisfacción de las personas, usuarios de los servicios de TI (55).

COBIT es el estándar generalmente aceptado que brinda buenas prácticas para gestión y control de las TI. COBIT está conformado por cuatro dominios, cada uno de los cuales están organizados en 34 procesos que se sub-dividen en actividades y objetivos de control (55).

Los procesos de estos dominios de COBIT se implantan dentro de las políticas y especificaciones de requerimientos de negocio, determinados por los criterios de la información, los cuales establecen los niveles de rendimiento en cada uno de los siguientes aspectos (55):

- Eficiencia/Eficacia
- Confidencialidad
- Integridad
- Disponibilidad
- Conformidad

Estos criterios deben ser tomados en cuanto al momento de ejecutar los procesos COBIT y al momento de monitorear los diversos recursos de TI con los que cuenta la compañía (aplicaciones, información, infraestructura y personas). Estos nos dan un marco completo de trabajo para gestionar y controlar las TI y poder maximizar los beneficios de las TI para con la organización (55).

Diferencias ITIL vs COBIT

Cervantes A. (56), muestra la siguiente diferencia:

- COBIT, evalúa, formula, define, justifica y audita, es más completo y sistemático.
- COBIT define qué debemos controlar e ITIL define cómo debemos hacerlo.

- COBIT sirve para planear, organizar, dirigir y controlar toda la función informática dentro de una Empresa.
- ITIL actúa sobre los procesos y, a través del conjunto de buenas prácticas que lo conforman, mejorar el servicio que ofrece la Empresa y medirlos para una mejora continua.
- ITIL mejores prácticas de prestación de servicios de TI; COBIT mejores prácticas en la administración de recursos de TI.
- COBIT herramienta de gobierno de TI que ayuda al entendimiento y a la administración de riesgos asociados con tecnología de información y con tecnologías relacionadas (56).

El gobierno de las TIC – COBIT

El gobierno de las TIC, es una estructura de relaciones y procesos para dirigir y controlar la Empresa con el propósito de alcanzar los objetivos de la Empresa y añadir valor mientras se balancean los riesgos sobre TIC y sus procesos (57).

COBIT habilita el desarrollo de una política clara y de buenas prácticas de control de TIC a través de organizaciones, a nivel mundial. El objetivo de COBIT es proporcionar estos objetivos de control, dentro del marco referencial definido, y obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo (58).

COBIT se orienta tanto a la gestión como al control y auditoría de TIC, facilitando las directrices de auditoría sobre una herramienta complementaria para la fácil aplicación del marco referencial y los objetivos de control COBIT dentro de las actividades de auditoría y evaluación. El propósito de las directrices de auditoría es contar con una estructura sencilla para auditar y evaluar controles, con base en

prácticas de auditoría generalmente aceptadas y compatibles con el esquema global COBIT (58).

Desde el punto de vista de gestión COBIT provee un conjunto de directrices gerenciales que son genéricas y que están orientadas a la acción con el fin de resolver los tipos siguientes de preocupaciones de la administración (54):

- Medición del desempeño - ¿Cuáles son los indicadores de un buen desempeño?
- Determinación del perfil de control de TIC ¿Qué es importante?
- El marco referencial de COBIT está estructurado en 04 dominios, 34 procesos y 300 objetivos de control. Cada uno de ellos puede ser tratado como variables y se utilizan en el presente estudio.

Figura N° 12: Gobierno de TIC- COBIT

Fuente: ISACA (52).

Seguridad Informática

Definimos la seguridad de información como la protección de ventajas de información de la revelación no autorizada, de la modificación, o de la destrucción, o accidental o intencional, o la incapacidad para procesar esa información. La seguridad de la red, se compone de esas medidas tomadas para proteger una red del acceso no autorizado, interferencia accidental o intencionada con operaciones normales, o con la

destrucción, inclusive la protección de facilidades físicas, del software, y de la seguridad del personal (59).

Objetivos de la Seguridad.

Seguridad informática es el conjunto de procedimientos, estrategias y herramientas que permitan garantizar la integridad, la disponibilidad y la confidencialidad de la información de una entidad (59):

Integridad.- Es necesario asegurar que los datos no sufran cambios no autorizados, la pérdida de integridad puede acabar en fraudes, decisiones erróneas o como paso a otros ataques. El sistema contiene información que debe ser protegida de modificaciones imprevistas, no autorizas o accidentales, como información de censo o sistemas de transacciones financieras.

Disponibilidad.- Se refiere a la continuidad operativa de la entidad, la pérdida de disponibilidad puede implicar, la pérdida de productividad o de credibilidad de la entidad. El sistema contiene información o proporciona servicios que deben estar disponibles a tiempo para satisfacer requisitos o evitar pérdidas importantes, como sistemas esenciales de seguridad y protección de la vida.

Confidencialidad.- Se refiere a la protección de datos frente a la difusión no autorizada, la pérdida de confidencialidad puede resultar en problemas legales, pérdida del negocio o de credibilidad. El sistema contiene información que necesita protección contra la divulgación no autorizada, como información parcial de informes, información personal o información comercial patentada (59).

Estrategias de Seguridad

La metodología de seguridad está diseñada para ayudar a los profesionales de la seguridad a desarrollar una estrategia para proteger la disponibilidad, integridad y confidencialidad de los datos de los sistemas informáticos (IT) de las organizaciones. Es de interés para los administradores de recursos de información, los directores de seguridad informática y los administradores, y tiene un valor especial para todos aquellos que intentan establecer directivas de seguridad.

La metodología ofrece un acercamiento sistemático a esta importante tarea y, como precaución final, también implica el establecimiento de planes de contingencia en caso de desastre.

Los administradores de seguridad tienen que decidir el tiempo, dinero y esfuerzo que hay que invertir para desarrollar las directivas y controles de seguridad apropiados (59).

Identificación y prevención de problemas de seguridad

La política de seguridad define lo que necesita protegerse, pero no señala explícitamente como deben protegerse los recursos y el enfoque general para manejar los problemas de seguridad. En una sección separada de la política de seguridad deben abordarse los procedimientos generales que deben implementarse para evitar problemas de seguridad (60).

La política de seguridad debe remitirse a la guía del administrador de sistemas del sitio respecto a detalles adicionales acerca de la implementación de los procedimientos de seguridad. Antes de establecer los procedimientos de seguridad, debe evaluar el nivel de importancia de los recursos de la red y su grado de riesgo. Si no se conocen adecuadamente los recursos más importantes y los que están expuestos a mayores riesgos, el enfoque anterior hará que ciertas áreas

tengan más protección de la que necesitan, y que otras áreas más importantes no tengan suficiente protección (60).

Establecer una política de seguridad eficaz requiere considerable esfuerzo. Se necesita cierto esfuerzo para considerar todos los aspectos y cierta disposición para establecer las políticas en papel y hacer lo necesario para que los usuarios de la red la entiendan adecuadamente.

Además de realizar el análisis de riesgo de los recursos de la red, usted debe identificar otros puntos vulnerables. La siguiente lista es un intento de describir algunas de las tareas más problemáticas. Esta lista lo puede orientar en la dirección correcta, pero de ningún modo está completa, ya que es probable que su sitio tenga algunos puntos vulnerables particulares (60).

- Puntos de acceso
- Sistemas configurados inadecuadamente
- Problemas de software
- Amenazas internas

III. METODOLOGÍA

3.1. Tipo de la investigación

Por las características la presente investigación tiene un enfoque cuantitativo ya que cumple la función de recoger y analizar una cierta cantidad de variables de estudio.

Según Guillermo (61), La investigación es cuantitativa ya que está basada en el paradigma explicativo, es decir, utiliza preferentemente información cuantitativa o cuantificable para describir o tratar de explicar los fenómenos que estudia, en las formas que es posible hacerlo en el nivel de estructuración lógica en el cual se encuentran las ciencias sociales actuales.

Para ello, según Galileo G. (62), afirmaba en este sentido "mide lo que sea medible y haz medible lo que no lo sea la investigación cuantitativa", mediante la cual es aquella que recoge información empírica (de cosas o aspectos que se pueden contar, pesar o medir) y que por su naturaleza siempre arroja números como resultado. Es fuerte en cuanto a la precisión del fenómeno mismo pero es débil en cuanto al papel del contexto o ambiente en la generación de esos datos.

3.2. Nivel de la investigación

De la misma forma el nivel de la investigación es descriptiva y explicativa, considerando descriptiva porque está caracterizada por conocer ciertas situaciones, procesos, actividades, que se adecuan al propósito de la investigación.

Plasencia J. (2), identifica la investigación descriptiva, porque su objetivo es llegar a conocer las situaciones, costumbres y actitudes predominantes

a través de la descripción exacta de las actividades, procesos y personas, examinando y describiendo las variables de estudio.

Sin embargo Bavaresco A. (63), hace mención que la investigación es descriptiva ya que mediante este tipo de investigación, utiliza el método de análisis, logrando caracterizar un objeto de estudio o una situación concreta, señalar sus características y propiedades, sirve para ordenar, agrupar o sistematizar los objetos involucrados en el trabajo indagatorio.

Para Víctor (64), las investigaciones explicativas son más estructuradas que las demás clases de estudios y de hecho implican los propósitos de todas ellas (exploración, descripción y correlación), además que proporcionan un sentido de entendimiento del fenómeno a que hacen referencia.

Por otro lado el tipo de investigación es explicativa, según lo escrito por Niño (65), cuando averigua las causas de las cosas, hechos o fenómenos de la realidad. La explicación es un proceso que va mucho más allá de la simple descripción de un objeto. Esta es más avanzada, es decir trata de explicar el porqué.

3.3. Diseño de la investigación

La investigación se caracteriza por ser no experimental, por lo que no manipulan variables que interfieren en el estudio, la cual es utilizada cuando el investigador no dispone de la información necesaria para solucionar el problema definido, para ello se plantean preguntas para estudiar los fenómenos tal cual se dan dentro de su contexto, para darle un análisis.

El diseño de la investigación es no experimental, según la Universidad de La Habana (66), cuando ésta se realiza sin manipular

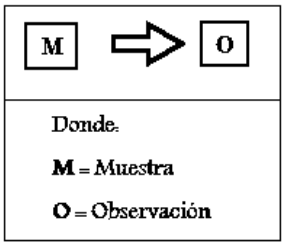
deliberadamente las variables independientes, se basa en variables que ya ocurrieron o se dieron en la realidad sin la intervención directa del investigador. Es un enfoque retrospectivo.

La característica de esta investigación será de corte transversal, porque se analizan los hechos en un periodo determinado, recolectando datos en tiempo único, para detallar las variables y sucesos en un momento dado, según el problema en estudio.

El diseño de la investigación es de corte transversal, según Mina (67), cuando la investigación se centra en analizar cuál es el nivel de una o diversas variables en un momento dado. También es adecuado para analizar la relación entre un conjunto de variables en un punto del tiempo. Puede abarcar varios grupos o subgrupos de personas, objetos o indicadores.

El diseño de la investigación se gráfica de la siguiente manera:

Figura N° 13: Diseño de Investigación



Fuente: Elaboración propia.

3.4. Población y muestra

Población: Actualmente cuenta con 60 trabajadores, mientras las áreas encargadas del manejo de la TIC están conformada por 27 trabajadores.

Muestra: El criterio de selección está compuesto mediante un muestreo no probabilístico, ya que tienen un factor común hacia la investigación,

por lo que se trabajó con un tamaño de muestra de 27 trabajadores, que son aquellas personas involucradas directamente en los procesos de las TIC, por lo que están compuestos en las siguientes áreas:

Tabla N° 4: División de trabajadores de ARCOPA S.A

Áreas	**Población**	**Muestra**
Gerencia General.	2	2
Gerencia de Secretaria General.	1	1
Administración.	8	5
Contabilidad.	9	4
Exportaciones.	10	4
Recursos Humanos.	6	3
Sistemas Informática.	1	1
Seguridad Industrial.	5	2
Operaciones	8	3
Planta de Harina	10	2
Total	**60**	**27**

Fuente: Elaboración propia, recopilación de datos de la Empresa ARCOPA S.A.

3.5. Plan de análisis

a. Operacionalización de variables

Tabla N° 5: Operacionalización de variables

Variable	Definición conceptual	Dimensiones	Indicadores	Escala de medición	Definición operacional
AUDITORÍA BASADA EN COBIT 4.1 PARA EL USO ÓPTIMO DE LAS TIC Y LA SEGURIDAD	Auditoría.- La auditoría es el examen organizado de una situación relativa a un producto, proceso u organización, en materia de calidad, realizado en cooperación con los interesados para verificar la concordancia de la realidad con lo preestablecido y la adecuación al objetivo buscado	Incrementar el nivel de seguridad de cada uno de los procesos de TIC que maneja la Empresa.	- Directrices para protección de toda la información. -Efectividad en la ejecución de sus proyectos. -Controles preventivos de adquisiciones e infraestructura.	-Nominal -Ordinal	Con referencia a la auditoría es muy importante examinar, verificar y analizar los procesos que mediante las TIC se ejecutan diversas tareas en dicha Empresa, ya que a través de ello se establecerá una guía de buenas prácticas como marco de trabajo de
		Mejorar el nivel de capacitación en temas de seguridad informática en el	- Conocimientos eficientes. - Buenas Prácticas en el área de tecnología.		

INFORMÁTICA	(8). Seguridad de TIC.- Conjunto de medidas de seguridad para proteger la información almacenada, procesada o transmitida por sistemas de información y telecomunicaciones, de manera que se preserve la confidencialidad, integridad y disponibilidad de la información y la integridad y la disponibilidad de los elementos que la tratan (41).	personal.	- Logro de producción de servicios en función a los recursos tecnológicos.		control y supervisión de TIC al objetivo buscado. La seguridad de las TIC en la Empresa ARCOPA S.A, permitirá proteger, procesar y transmitir la información protegida y almacenada, para preservar la confidencialidad, integridad y disponibilidad de los elementos que la tratan.
		Disminuir los niveles de riesgos, detectar anomalías en la seguridad informática, amenazas y vulnerabilidades.	-Identificar fallas de los equipos de cómputo. -Revisión de las exigencias de seguridad de los equipos de cómputo. -Establecimiento de un ambiente separado para pruebas		

Fuente: Elaboración propia.

b. Técnicas e instrumentos

Arias F. (68), menciona que las técnicas de recolección de datos son las estrategias que utiliza el investigador para recolectar información, para la aplicación de la estrategia de investigación a seguir.

Dentro de los primordiales instrumentos para realizar esta Auditoría se utilizó la siguiente estrategia:

1. Encuesta: Las encuestas se basan en un test escrito realizado para obtener información de población interesa, para llevar a cabo una investigación más profunda.

2. Cuestionarios.- Es el conjunto de preguntas que se pueden responder oralmente o escrito de acuerdo al conjunto de variables que se pretende medir en la investigación.

3. Observación: Analiza un conjunto de datos propios del suceso que se investiga.

c. Procedimiento de recolección de datos

Para lograr la recolección de datos de la Empresa pesquera ARCOPA S.A, según los indicadores correspondientes, es el siguiente: Se ha solicitado por escrito una solicitud dirigida al Sr. Gerente General, para que brinde la autorización de realizar este proyecto de investigación y así poder acceder a la información necesaria para la realización del estudio.

d. Plan de análisis de datos

Los datos que se obtendrán serán codificados e ingresados en una hoja de cálculo usando el programa Microsoft Professional Excel 2016, la cual se analizarán los datos y se presentarán los resultados de las variables en estudio.

3.5. Matriz de consistencia

Tabla N° 6: Matriz de consistencia

PROBLEMA	OBJETIVO	HIPÓTESIS	METODLOGÍA	VARIABLE
¿De qué manera beneficia la auditoría basada en COBIT 4.1, para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A.?	**Objetivo general:** Implementar una auditoría basada COBIT 4.1, para el uso óptimo las TIC y la seguridad informática la Empresa ARCOPA S.A. **Objetivos específicos:** * Incrementar el nivel de seguridad de los procesos de TIC de la Empresa ARCOPA S.A. * Capacitar al personal involucrado en TIC sobre la	**Hipótesis general** La Auditoría basada en COBIT 4.1, para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A., logrará minimizar riesgos, haciendo uso de técnicas y estrategias de análisis, evaluando controles para el buen uso y normal funcionamiento de las tecnologías de información	**Tipo de la investigación** • Cuantitativa **Nivel de la investigación** • Descriptiva • Explicativa **Diseño de la investigación** • No experimental • Corte transversal	Auditoría basada en COBIT 4. para el uso óptimo de las TIC y seguridad informática

	Seguridad informática. * Analizar, evaluar y diagnosticar la situación actual con respecto a los marcos de referencia y control interno para obtener un sistema que permita crear un ambiente seguro de las TIC.	de la Empresa Pesquera ARCOPA S.A.		

Fuente: Elaboración propia

3.6. Principios Éticos

Durante el desarrollo de la presente investigación denominada "Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática, se ha estimado de manera rígida el cumplimiento de los principios éticos que permitan asegurar la originalidad de la Investigación. De la misma forma, se han respetado los derechos de propiedad intelectual de los libros de texto y de las fuentes electrónicas consultadas, necesarias para estructurar el marco teórico.

Por otro lado, considerando que gran parte de los datos utilizados son de carácter público, y pueden ser conocidos y empleados por diversos analistas sin mayores restricciones, se ha incluido su contenido sin modificaciones, salvo aquellas necesarias por la aplicación de la metodología para el análisis requerido en esta investigación.

Igualmente, se conserva intacto el contenido de las respuestas, manifestaciones y opiniones recibidas de los trabajadores y funcionarios que han colaborado contestando las encuestas a efectos de establecer la relación causa-efecto de la o de las variables de investigación. Finalmente, se ha creído conveniente mantener en reserva la identidad de los autores con la finalidad de lograr objetividad en los resultados.

IV. RESULTADOS

4.1. Dimensión 01.- Nivel de madurez de los procesos de seguridad para la eficiencia, eficacia, confiabilidad de las Tecnologías de Información y Comunicación.

Tabla N° 7: Existencia de manuales

Distribución de frecuencias y respuestas relacionadas con la existencia de manuales; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	8	29.63
No	19	70.37
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿El área de informática cuenta con un manual de organización y funciones?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 7 se puede visualizar que el 70.37% de los trabajadores encuestados expresaron que NO cuenta con un manual de organización y funciones, por lo tanto, el 29.63% de los trabajadores encuestados indicó que sí.

Tabla N° 8: Existencia de métodos

Distribución de frecuencias y respuestas relacionadas con la existencia de métodos; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	5	18.52
No	22	81.48
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Se tienen identificados los archivos con información confidencial y se cuenta con claves de acceso?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 8 se puede visualizar que el 81.48% de los trabajadores encuestados expresaron que NO identifican los archivos con información confidencial y algunas cuentas no cuentan con claves de acceso, por lo tanto, el 18.52% de los trabajadores encuestados indicó que sí.

Tabla N° 9: Procedimientos establecidos

Distribución de frecuencias y respuestas relacionadas con los procedimientos establecidos; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	5	18.52
No	22	81.48
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Se tienen establecidos procedimientos de actualización para estas copias de archivos?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 9 se puede visualizar que el 81.48% de los trabajadores encuestados expresaron que NO tienen establecidos procedimientos de actualización para estas copias de archivos, por lo tanto, el 18.52% de los trabajadores encuestados indicó que sí.

Tabla N° 10: Procesos definidos

Distribución de frecuencias y respuestas relacionadas con procesos claramente definidos; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	10	37.04
No	17	62.96
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Se tiene definido algún proceso para monitorear, evaluar y administrar el recurso humano de TI?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 10 se puede visualizar que el 62.96% de los trabajadores encuestados expresaron que NO tiene definido algún proceso para monitorear, evaluar y administrar el recurso humano de TI, por lo tanto, el 37.04% de los trabajadores encuestados indicó que sí.

Tabla N° 11: Registro de accesos

Distribución de frecuencias y respuestas relacionadas con el respectivo registro de acceso; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	9	33.33
No	18	66.67
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Se registra el acceso al centro de datos de personas ajenas al área de cómputo?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 11 se puede visualizar que el 66.67% de los trabajadores encuestados expresaron que NO se registra el acceso al centro de datos de personas ajenas al área de cómputo, por lo tanto, el 33.33% de los trabajadores encuestados indicó que sí.

Tabla N° 12: Medidas preventivas y correctivas

Distribución de frecuencias y respuestas relacionadas con las medidas preventivas y correctivas; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	7	25.93
No	20	74.07
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Existen medidas preventivas y correctivas de planes tácticos existentes en la Empresa?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 12 se puede visualizar que el 74.07% de los trabajadores encuestados expresaron que NO existen medidas preventivas y correctivas de planes tácticos existentes en la Empresa, por lo tanto, el 25.93% de los trabajadores encuestados indicó que sí.

Tabla N° 13: Controles

Distribución de frecuencias y respuestas relacionadas con los diversos controles; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	10	37.04
No	17	62.96
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Existe un control estricto de las copias de estos archivos?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 13 se puede visualizar que el 62.96% de los trabajadores encuestados expresaron que NO existe un control estricto de las copias de estos archivos, por lo tanto, el 37.04% de los trabajadores encuestados indicó que sí.

Tabla N° 14: Seguridad de almacenamiento

Distribución de frecuencias y respuestas relacionadas con la seguridad de almacenamiento; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	20	74.07
No	7	25.93
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 14 se puede visualizar que el 74.07% de los trabajadores encuestados expresaron que SI están satisfechos que se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado, por lo tanto, el 25.93% de los trabajadores encuestados indicó que no.

Tabla N° 15: Planificación estratégica

Distribución de frecuencias y respuestas relacionadas con la planificación estratégica; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	4	14.81
No	23	85.19
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Se ha realizado una planificación estratégica del sistema de información para la Empresa?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 15 se puede visualizar que el 85.19% de los trabajadores encuestados expresaron que NO se ha realizado una planificación estratégica del sistema de información, por lo tanto, el 14.81% de los trabajadores encuestados indicó que sí.

Tabla N° 16: Cronogramas de mantenimiento

Distribución de frecuencias y respuestas relacionadas con la ejecución de cronogramas de mantenimiento; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	--	--
No	27	100.00
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 16 se puede visualizar que el 100% de los trabajadores encuestados expresaron que NO Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo.

Tabla N° 17: Dimensión Nivel de madurez de los procesos de seguridad para la eficiencia, eficacia, confiabilidad de las TIC.

Distribución de frecuencias y respuestas relacionadas con la Dimensión N°01: Nivel de madurez de los procesos de seguridad para la eficiencia, eficacia, confiabilidad de las TIC de la Empresa ARCOPA S.A. Paita; 2017

Dimensión N° 01	n	%
Si	10.50	38.89
No	16.50	61.11
Total	27	100.00

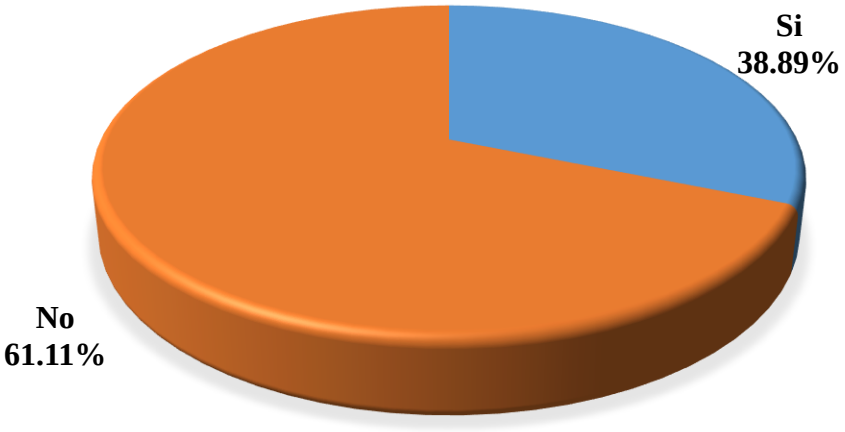
Fuente: Origen del cuestionario aplicado a trabajadores Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para desarrollar una Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 17 se puede apreciar que el 61.11% de los trabajadores encuestados concluyeron que NO se maneja un pleno control en cada uno de los procesos de seguridad para la eficiencia, eficacia, confiabilidad de las TIC en la Empresa y es por ello que están satisfactoriamente de acuerdo que al aplicar la Auditoría será de gran beneficio para mejorar la seguridad en cada uno de sus procesos de toda la organización, mientras que el 38.89% indicó que los procesos SI se controlan.

Gráfico Nro. 10: Nivel de madurez de los procesos de seguridad para la eficiencia, eficacia, confiabilidad de las TIC.

Distribución porcentual de las frecuencias y respuestas relacionadas con la Dimensión N° 01: Nivel de madurez de los procesos de seguridad para la eficiencia, eficacia, confiabilidad de las TIC., para desarrollar una Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.



Fuente: Tabla N° 17

4.2. Dimensión 02.- Nivel de madurez en los grados de conocimiento acerca de los niveles de las operaciones de trabajo de las Tecnologías de Información y Comunicación.

Tabla N° 18: Capacitaciones

Distribución de frecuencias y respuestas relacionadas con las diversas capacitaciones en TIC; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	--	--
No	27	100.00
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Se da algún tipo de inducción al personal para que este informado de las funciones que realizará?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 18 se puede visualizar que el 100% de los trabajadores encuestados expresaron que NO se realizan inducciones al personal sobre las funciones que realizará.

Tabla N° 19: Reglamentos de TIC

Distribución de frecuencias y respuestas relacionadas con los reglamentos de TIC; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	5	18.52
No	22	81.48
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Conoces el reglamento implementado dentro del centro de cómputo?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 19 se puede visualizar que el 81.48% de los trabajadores encuestados expresaron que NO conocen el reglamento implementado dentro del centro de cómputo, por lo tanto, el 18.52% de los trabajadores encuestados indicó que sí.

Tabla N° 20: Políticas de TIC

Distribución de frecuencias y respuestas relacionadas con las políticas de TIC; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	3	11.11
No	24	88.89
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Cumples con los reglamentos y políticas estipuladas dentro del centro de cómputo?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 20 se puede visualizar que el 88.89% de los trabajadores encuestados expresaron que NO se cumplen con los reglamentos y políticas estipuladas dentro del centro de cómputo, por lo tanto, el 11.11% de los trabajadores encuestados indicó que sí.

Tabla N° 21: Competencias y habilidades

Distribución de frecuencias y respuestas relacionadas con la competencias y habilidades; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	10	37.04
No	17	62.96
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿El personal de la Unidad de TI posee las competencias y habilidades adecuadas para realizar su función?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 21 se puede visualizar que el 62.96% de los trabajadores encuestados expresaron que NO están satisfechos con el personal de la Unidad de TI, por lo que no posee competencias y habilidades adecuadas para realizar su función, por lo tanto, el 37.04% de los trabajadores encuestados indicó que sí.

Tabla N° 22: Cumplimiento del plan de trabajo

Distribución de frecuencias y respuestas relacionadas el cumplimiento del plan de trabajo; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	4	14.81
No	23	85.19
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Se recibe retroalimentación de la Administración acerca del cumplimiento del plan de trabajo de la Unidad de TI?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 22 se puede visualizar que el 85.19% de los trabajadores encuestados expresaron que NO se recibe retroalimentación de la Administración acerca del cumplimiento del plan de trabajo de la Unidad de TI, por lo tanto, el 14.81% de los trabajadores encuestados indicó que sí.

Tabla N° 23: Satisfacción del usuario

Distribución de frecuencias y respuestas relacionadas con la satisfacción del usuario; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	8	29.63
No	19	70.37
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Se tiene información del nivel de satisfacción del usuario respecto a los servicios brindados?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 23 se puede visualizar que el 70.37% de los trabajadores encuestados expresaron que NO se hay satisfacción del usuario respecto a los servicios brindados, por lo tanto, el 29.63% de los trabajadores encuestados indicó que sí.

Tabla N° 24: Mecanismos de incidentes

Distribución de frecuencias y respuestas relacionadas con mecanismos de incidentes; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	5	18.52
No	22	81.48
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Se ha establecido un mecanismo para la atención de incidentes de seguridad de la información?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 24 se puede visualizar que el 81.48% de los trabajadores encuestados expresaron que NO se ha establecido un mecanismo para la atención de incidentes de seguridad de la información, por lo tanto, el 18.52% de los trabajadores encuestados indicó que sí.

Tabla N° 25: Protección de los equipos informáticos

Distribución de frecuencias y respuestas relacionadas con la protección de los equipos informáticos; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	5	18.52
No	22	81.48
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Se aplican mecanismos para garantizar la protección de los equipos informáticos?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 25 se puede visualizar que el 81.48% de los trabajadores encuestados expresaron que NO se aplican mecanismos para garantizar la protección de los equipos informáticos, por lo tanto, el 18.52% de los trabajadores encuestados indicó que sí.

Tabla N° 26: Restricciones

Distribución de frecuencias y respuestas relacionadas con las diversas restricciones de TIC; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	10	37.04
No	17	62.96
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Se cuenta con reglamento para el usuario y personal?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 26 se puede visualizar que el 62.96% de los trabajadores encuestados expresaron que NO cuenta con reglamentos para el usuario y personal, por lo tanto, el 37.04% de los trabajadores encuestados indicó que sí.

Tabla N° 27: Agilidad toma de decisiones

Distribución de frecuencias y respuestas relacionadas con la Agilidad toma de decisiones; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	8	29.63
No	19	70.37
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Permiten los niveles actuales que se tenga una ágil de toma de decisiones y comunicación ascendente y descendente?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 27 se puede visualizar que el 70.37% de los trabajadores encuestados expresaron que NO están satisfechos con la una agilidad de toma de decisiones y comunicación ascendente y descendente, por lo tanto, el 29.63% de los trabajadores encuestados indicó que sí.

Tabla N° 28: Dimensión Nivel de madurez en los grados de conocimiento acerca de los niveles de las operaciones de trabajo de las TIC.

Distribución de frecuencias y respuestas relacionadas con la Dimensión N°02: Nivel de madurez en los grados de conocimiento acerca de los niveles de las operaciones de trabajo de las TIC de la Empresa ARCOPA S.A. Paita; 2017

Dimensión N° 02	n	%
Si	8.4	31.1
No	18.5	68.5
Total	27	100

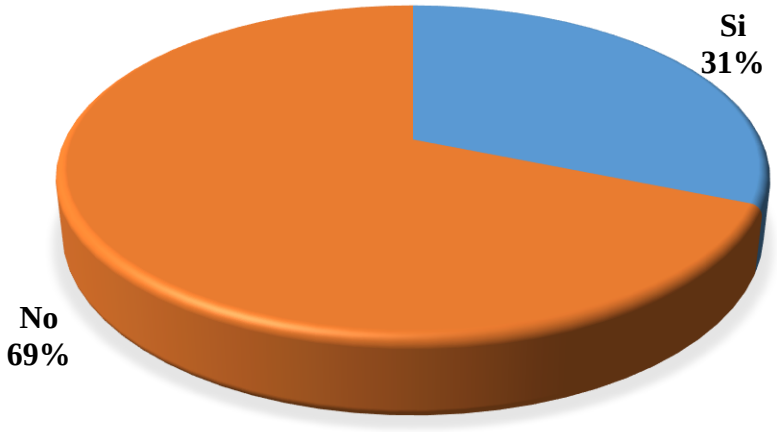
Fuente: Origen del cuestionario aplicado a trabajadores Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para desarrollar una Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 28 se puede apreciar que el 68.5% de los trabajadores encuestados concluyeron que NO mantienen un nivel de madurez alta en el conocimiento de niveles de las operaciones de trabajo de las TIC en la Empresa y se encuentran satisfactoriamente de acuerdo que al aplicar la Auditoría será de gran beneficio para mejorar la seguridad en cada uno de sus procesos de toda la organización, mientras que el 31.1% indicó que SI tienen conocimiento.

Gráfico Nro. 11: Nivel de madurez en los grados de conocimiento acerca de los niveles de las operaciones de trabajo de las TIC.

Distribución porcentual de las frecuencias y respuestas relacionadas con la Dimensión N° 02: Nivel de madurez de los procesos de seguridad para la eficiencia, eficacia, confiabilidad de las TIC., para desarrollar una Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.



Fuente: Tabla N° 28

4.3. Dimensión 03.- Nivel de madurez en los grados de evaluación de las operaciones de trabajo de las TIC.

Tabla N° 29: Evaluación operacional

Distribución de frecuencias y respuestas relacionadas con manuales funcionales; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	9	33.33
No	18	66.67
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿El área de informática evalúa cada una de las operaciones que se ejecutan dentro de la empresa?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 29 se puede visualizar que el 66.67% de los trabajadores encuestados expresaron que el área de informática NO área de informática no efectúa las diversos operaciones que se ejecutan en la empresa, por lo tanto, el 33.33% de los trabajadores encuestados indicó que sí.

Tabla N° 30: Plan de Seguridad

Distribución de frecuencias y respuestas relacionadas con un plan de seguridad; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	2	7.41
No	25	92.59
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿El área de informática cuenta con un plan de seguridad contra pérdida de datos?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 30 se puede visualizar que el 92.59% de los trabajadores encuestados expresaron que el área de informática NO cuenta con un plan de seguridad contra pérdida de datos, por lo tanto, el 7.41% de los trabajadores encuestados indicó que sí.

Tabla N° 31: Acciones operativas

Distribución de frecuencias y respuestas relacionadas con diversas acciones operativas; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	10	37.04
No	17	62.96
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 31 se puede visualizar que el 62.96% de los trabajadores encuestados expresaron que NO se registran las acciones de los operadores, por lo tanto, el 37.04% de los trabajadores encuestados indicó que sí.

Tabla N° 32: Informes técnicos

Distribución de frecuencias y respuestas relacionadas con la existencia de informes técnicos de TIC; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	3	11.11
No	24	88.89
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Existe un informe técnico en el que se justifique la adquisición del equipo, software y servicios de computación, incluyendo un estudio costo-beneficio?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 32 se puede visualizar que el 88.89% de los trabajadores encuestados expresaron que NO existen informes técnicos que justifique la adquisición de TI, por lo tanto, el 11.11% de los trabajadores encuestados indicó que sí.

Tabla N° 33: Equipos

Distribución de frecuencias y respuestas relacionadas con la satisfacción con respecto al servicio de equipos tecnológicos; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	8	29.63
No	19	70.37
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Existen políticas establecidas sobre el mantenimiento de los equipos?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 33 se puede visualizar que el 70.37% de los trabajadores encuestados expresaron que NO existen políticas establecidas sobre el mantenimiento de los equipos, por lo tanto, el 29.63% de los trabajadores encuestados indicó que sí.

Tabla N° 34: Manuales de Usuario

Distribución de frecuencias y respuestas relacionadas con los manuales de usuario; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	7	25.93
No	20	74.07
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿El área de informática cuenta con un manual del usuario por sistema?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 34 se puede visualizar que el 74.07% de los trabajadores encuestados expresaron que el área de informática NO cuenta con un manual del usuario por sistema, por lo tanto, el 25.93% de los trabajadores encuestados indicó que sí.

Tabla N° 35: Ejecución de Procesos

Distribución de frecuencias y respuestas relacionadas con la ejecución de procesos de TIC; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	4	14.81
No	23	85.19
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿El área de informática cuenta con procedimientos específicos que indiquen al operador qué hacer cuando un programa interrumpe su ejecución u otras dificultades en proceso?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 35 se puede visualizar que el 85.19 % de los trabajadores encuestados expresaron que NO cuentan con procedimientos específicos que indiquen al operador qué hacer cuando un programa interrumpe su ejecución u otras dificultades en proceso, por lo tanto, el 14.81% de los trabajadores encuestados indicó que sí.

Tabla N° 36: Procedimientos de reconstrucción

Distribución de frecuencias y respuestas relacionadas con los procedimientos de reconstrucción; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	9	33.33
No	18	66.67
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Se tienen procedimientos que permitan la reconstrucción de un archivo en cinta o disco, el cual fue inadvertidamente destruido?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 36 se puede visualizar que el 66.67% de los trabajadores encuestados expresaron que NO tienen procedimientos que permitan la reconstrucción de un archivo, por lo tanto, el 33.33% de los trabajadores encuestados indicó que sí.

Tabla N° 37: Funciones y responsabilidades

Distribución de frecuencias y respuestas relacionadas con la funciones y responsabilidades; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	5	18.52
No	22	81.48
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Están definidas formalmente las funciones y responsabilidades de la Unidad de TI?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 37 se puede visualizar que el 81.48% de los trabajadores encuestados expresaron que NO están definidas formalmente las funciones y responsabilidades de la Unidad de TI, por lo tanto, el 18.52% de los trabajadores encuestados indicó que sí.

Tabla N° 38: Plan de trabajo

Distribución de frecuencias y respuestas relacionadas con el plan de trabajo; respecto a la Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Alternativas	n	%
Si	10	37.04
No	17	62.96
Total	27	100.00

Fuente: Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para responder a la pregunta: ¿Se deja evidencia formal del plan de trabajo, los cambios realizados y la supervisión ejercida?

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 38 se puede visualizar que el 62.96% de los trabajadores encuestados expresaron que NO se deja evidencia formal del plan de trabajo, los cambios realizados y la supervisión ejercida, por lo tanto, el 37.04% de los trabajadores encuestados indicó que sí.

Tabla N° 39: Dimensión Nivel de madurez en los grados de evaluación de las operaciones de trabajo de las TIC.

Distribución de frecuencias y respuestas relacionadas con la Dimensión N°03: Nivel de madurez en los grados de evaluación de las operaciones de trabajo de las TIC de la Empresa ARCOPA S.A. Paita; 2017

Dimensión N° 03	n	%
Si	6.7	24.81
No	20.3	75.19
Total	27	100

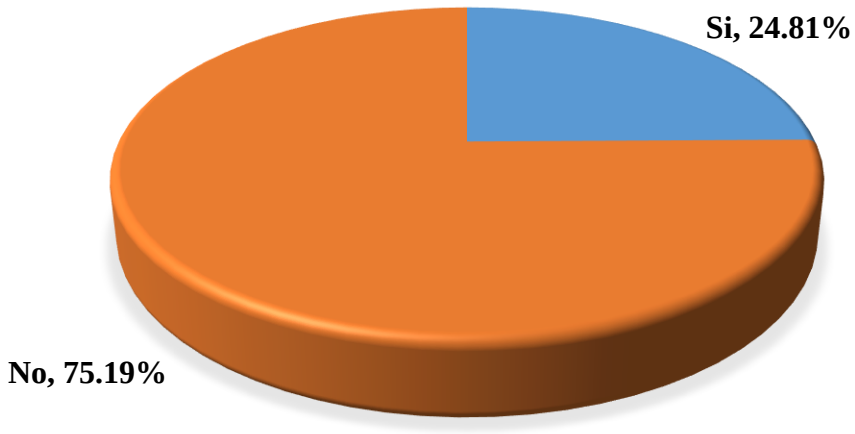
Fuente: Origen del cuestionario aplicado a trabajadores Origen del instrumento aplicado a los trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.; para desarrollar una Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 39 se puede apreciar que el 75.19% de los trabajadores encuestados concluyeron que NO cumplen con los grados de evaluación de las operaciones de trabajo de las TIC de la Empresa, es por ello que están satisfactoriamente de acuerdo que al aplicar la Auditoría será de gran beneficio para mejorar la seguridad en cada uno de sus procesos de toda la organización, mientras que el 24.81% indicó que si cumplen con las diversas operaciones de TIC.

Gráfico Nro. 12: Nivel de madurez en los grados de conocimiento acerca de los niveles de las operaciones de trabajo de las TIC.

Distribución porcentual de las frecuencias y respuestas relacionadas con la Dimensión N° 03: Nivel de madurez de los procesos de seguridad para la eficiencia, eficacia, confiabilidad de las TIC, para desarrollar una Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.



Fuente: Tabla N° 39

Tabla N° 40: Resumen General por Dimensiones

Distribución de frecuencias y respuestas relacionadas con las tres dimensiones tres dimensiones definidas para determinar el desarrollo de una Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.

Dimensiones	**Si**		**No**		**Total**	
	n	**%**	**n**	**%**	**n**	**%**
Dimensión Nivel de madurez de los procesos de seguridad	10.5	39	16.5	61	27	100
Dimensión Nivel de madurez de los grados de conocimiento	8	31	19	69	27	100
Dimensión Nivel de madurez en los grados de evaluación de las operaciones de trabajo de las TIC	7	25	20	75	27	100

Fuente: Origen del cuestionario aplicado a trabajadores involucrados directamente en los procesos de las TIC – ARCOPA S.A; 2017.

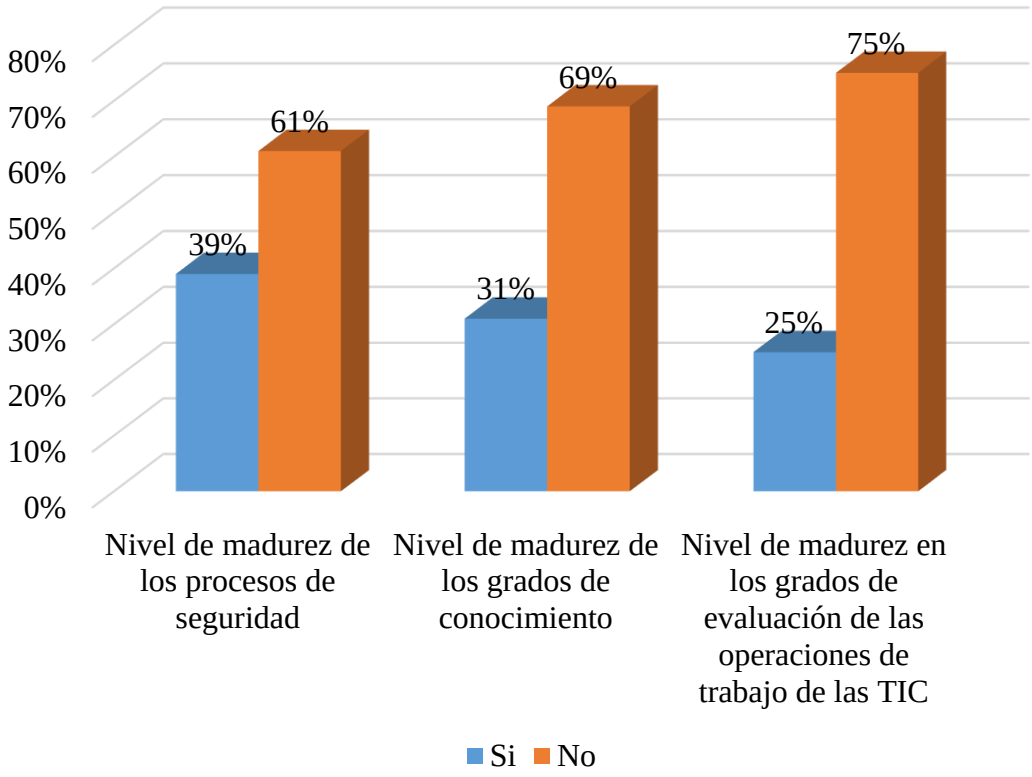
Aplicado por: Pangalima, R.; 2017.

En la Tabla N° 40 se puede apreciar los resultados porcentuales de cada una de las dimensiones, a la cual los trabajadores de la Empresa ARCOPA S.A. de Paita respondieron a las preguntas propuestas en el cuestionario, teniendo como resultado:

En lo que respecta la Dimensión N° 01 el 61% de los trabajadores encuestados NO se maneja un pleno control en cada uno de los procesos de seguridad para la eficiencia, eficacia, confiabilidad de las TIC en la Empresa y es por ello que están satisfactoriamente de acuerdo que al aplicar la Auditoría será de gran beneficio para mejorar la seguridad en cada uno de sus procesos de toda la organización, mientras que el 39% índico que sí, mientras tanto en la Dimensión N° 02 el 69% de los trabajadores encuestados concluyen que NO mantienen un nivel de madurez alta en el conocimiento de niveles de las operaciones de trabajo de las TIC en la Empresa y se encuentran satisfactoriamente de acuerdo que al aplicar la Auditoría será de gran beneficio para mejorar la seguridad en cada uno de sus procesos de toda la organización, mientras que el 31% índico que sí, finalmente en la Dimensión N° 03 el 75% de los trabajadores encuestados concluyeron que NO cumplen con los grados de evaluación de las operaciones de trabajo de las TIC de la Empresa, es por ello que están satisfactoriamente de acuerdo que al aplicar la Auditoría será de gran beneficio para mejorar la seguridad en cada uno de sus procesos de toda la organización, mientras que el 25% índico que sí.

Gráfico Nro. 11: Resumen general de dimensiones

Distribución porcentual de las frecuencias y respuestas relacionadas con las tres dimensiones definidas para determinar los niveles de satisfacción de los trabajadores para el desarrollo de Auditoría basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A. Paita; 2017.



Fuente: Tabla N° 40

4.4. Análisis de resultados

El objetivo principal de la presente investigación fue: Implementar la Auditoría basada en COBIT 4.1, para el uso óptimo de las TIC y la seguridad informática en la empresa ARCOPA S.A de Paita, es por ello que para llegar a cumplir con este objetivo, es de suma importancia efectuar una evaluación intensa de la situación actual de la Empresa, con la finalidad de que esta investigación identifique claramente los procesos de estudio y pueda cubrir cada una de las exigencias de la Empresa a través de un plan de mejora compuesta y técnica.

Para ello se plasmó una encuesta asociada en 03 dimensiones, teniendo en cuenta que se ha obtenido resultados e interpretación, se alcanza realizar el siguiente análisis:

1. En la relación a la Dimensión N° 01: "Nivel de madurez de los procesos de seguridad para la eficiencia, eficacia, confiabilidad de las TIC", con respecto a la implementación de una auditoría, en la Tabla N° 17, identifica que el 61.11% de los trabajadores encuestados concluyeron que NO se maneja un pleno control en cada uno de los procesos de seguridad para la eficiencia, eficacia, confiabilidad de las TIC en la Empresa y es por ello que están satisfactoriamente de acuerdo que al aplicar la Auditoría será de gran beneficio para mejorar la seguridad en cada uno de sus procesos de toda la organización, a comparación con los resultados obtenidos en la investigación realizada por Villegas M., en el año 2009 (3), en su artículo: "Modelo de Madurez de la Gestión de la Seguridad Informática en el contexto de las Organizaciones Inteligentes", ofrece una propuesta de un modelo de madurez para la Gestión de la Seguridad de la Información partiendo del punto de vista de las Organizaciones Venezuela Inteligentes, las cuales se enmarcan en cinco disciplinas: el dominio personal, los modelos mentales, la visión compartida, el aprendizaje

en equipo y el pensamiento sistémico, esto se justifica porque en ambos resultados se busca disminuir la complejidad y la incertidumbre en la gestión de la seguridad la TIC en las organizaciones lo que contribuirá a la fácil identificación de las problemas para proteger los activos informáticos.

2. En relación a la Dimensión N° 02: "Nivel de madurez en los grados de conocimiento acerca de los niveles de las operaciones de trabajo de las TIC", con respecto a la implementación de una auditoría, en la Tabla N° 28 se puede apreciar que el 69% de los trabajadores encuestados concluyeron que NO mantienen un nivel de madurez alta en el conocimiento de niveles de las operaciones de trabajo de las TIC en la Empresa, a comparación con los resultados obtenidos en la investigación realizada por Choque R. (7), en el año 2009, en su tesis doctoral: Estudio en aulas de innovación pedagógica y desarrollo de capacidades TIC en los estudiantes de educación secundaria de la Red Educativa N° 11de la UGEL San Juan de Lurigancho, concluyó que el estudio en las Aulas de Innovación Pedagógica mejora el desarrollo de capacidades TIC, puesto que los estudiantes en contacto con las nuevas TIC como la computadora y el Internet tienen efectos en su capacidad de su intelecto humano, puesto que aprenden de la tecnología ciertas capacidades tecnológicas que son cambios permanentes que se dan en los estudiantes, esto se justifica porque en ambos resultados se evidencia que hoy en día se debe tener la mayor capacidad para llevar un buen manejo de las TIC para así lograr mejorar la seguridad en cada uno de sus procesos de toda la organización.

3. En lo que concierne a la Dimensión N° 03: "Nivel de madurez en los grados de evaluación de las operaciones de trabajo de las TIC", con respecto a la implementación de una auditoría, en la Tabla N° 39 nos muestra los resultados donde se determina que el 75.19% de los

trabajadores encuestados concluyeron que NO cumplen con los grados de evaluación de las operaciones de trabajo de las TIC de la Empresa, a comparación con los resultados obtenidos en la investigación realizada por Vera (6) en el año 2010, en su tesis para la obtención del Grado de Magíster: Competencia en tecnologías de información y comunicación en docentes del área de comunicación de Instituciones educativas de la región Callao, Perú, concluyó que el 42% de los docentes encuestados del área de comunicación se encuentra en el nivel medio en los grados de las operaciones que se manejan en las TIC, esto se justifica porque en ambos resultados tienen la necesidad de obtener una evaluación para mejorar la seguridad en cada uno de sus procesos de toda la organización.

4.5. Propuestas de Mejora

4.5.1. Propuesta Técnica

Al observar los resultados de la presente investigación, se ha comprendido el análisis y la evaluación para ejecutar una auditoría basada en COBIT 4.1, para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A., la cual se identificará soluciones para reducir riesgos y alcanzar la eficiencia en las TIC para una adecuada toma de decisiones de confiabilidad en su infraestructura e información, en el entorno de la seguridad lógica y física de las TIC, administrando medidas de seguridad tecnológicas, cumpliendo propósitos de las cuales han sido creadas.

Al analizar y evaluar los niveles de madurez en cada uno de sus procesos, se consideró que la empresa se encuentra en el Nivel 2.- Repetible, la cual no hay entrenamiento, información formal de procedimientos documentados de las actividades establecidas, ya

que mantienen un alto grado de confianza del conocimiento de los trabajadores, es por ello que los errores sean más probables.

Es por ello que se tiene en cuenta lo siguiente:

Establecer los lineamientos para el control y buen uso de los sistemas de cómputo, programas (software), servicios informáticos (internet, correo electrónico, etc.), integridad de la información electrónica, sistemas de copiado e impresión de la empresa ARCOPA S.A.

Los usuarios son responsables de cumplir con todas las políticas de ARCOPA S.A. relativas a la seguridad informática y en particular.

1. Alcance

A todo el personal de ARCOPA S.A. que tenga bajo su responsabilidad y resguardo, sistemas de cómputo, programas (software), servicios informáticos (internet, correos electrónicos, etc.), integridad de la información electrónica, sistemas de copiado e impresiones y demás bienes informáticos de la empresa.

2. Aplicación de esta Política

El cumplimiento de la presente política es obligatorio para todos los usuarios de ARCOPA S.A. en cualquiera de sus ubicaciones físicas.

ARCOPA S.A. designa al área de Sistemas e Informática como responsable a lo estipulado en el presente:

- Advertencia al usuario.

- Notificación al jefe inmediato superior del usuario, y al responsable de RRHH.
- Restricción o suspensión de los servicios.

3. Políticas de Seguridad General

- No divulgar información confidencial de la compañía a personas no autorizadas.
- No permitir y no facilitar el uso de los sistemas informáticos de la compañía a personas no autorizadas.
- No se permite la interconexión a la red interna de la empresa a toda aquella persona que no sea funcionario de la misma. Con la salvedad de funcionarios externos que provengan de entes de control, auditoría, funcionarios del grupo empresarial, entre otros, con autorización de la Gerencia.
- No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones para otras actividades que no estén directamente relacionadas con el trabajo en la empresa.
- Proteger su contraseña y evitar que sea vista por otras personas en forma inadvertida.
- Reportar inmediatamente a su jefe inmediato y al responsable del Departamento de Sistemas e Informática cualquier evento que pueda comprometer la seguridad de la empresa y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades inusuales.

4. Políticas de Seguridad para Computadores

- Los computadores de ARCOPA S.A. sólo deben usarse en un ambiente seguro. Se considera que un ambiente es

seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos.

- Es responsabilidad de los usuarios, velar por el aseo y protección de los equipos de trabajo; esto incluye limpieza de las zonas donde se encuentran instalados los equipos, utilizar medios de protección contra el polvo, agua, incendio.
- Los equipos de ARCOPA S.A. solo deben usarse para actividades de trabajo y no para otros fines.
- No modificar la configuración de hardware y software establecida por el departamento de sistemas e Informática.
- Como medida de higiene y de seguridad del equipo físico (hardware), queda totalmente prohibido el fumar, ingerir bebidas o alimentos mientras se esté utilizando los equipos de cómputo, ya que este tipo de práctica pone en riesgo el buen funcionamiento de los mismos.
- Como medida de protección, queda prohibido dejar objetos sobre los equipos de cómputo, ya que esto puede ocasionar accidentes (sobrecalentamiento de los equipos, ocasionando cortos internos, daños del procesador, daño en los discos duros, de la memoria RAM) y bajas en el rendimiento de los mismos, evidenciando un deterioro progresivo en los equipos.
- Será responsabilidad del usuario encargado del equipo de trabajo; el velar por el buen funcionamiento y cuidado del computador; por lo tanto si este último llegase a quebrantar negligentemente la política 5 y 6 recaerán sobre este todas las acciones pertinentes.
- No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la compañía se requiere

autorización de Gerencia General y presentarlo en Garita con las respectivas firmas y guías de salida.

- La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente a los responsables del Departamento de Sistemas e Informática.
- No está permitido llevar al sitio de trabajo computadores portátiles personales y en caso de ser necesario se requiere solicitar la autorización.
- Los usuarios no deben copiar a un medio removible (como un diskette, CD-ROM, memorias USB, dispositivos de almacenamiento masivo), el software o los datos residentes en los computadores de ARCOPA S.A., para ser trasladados fuera de las instalaciones, sin la aprobación previa de Gerencia General y departamento de Sistemas e Informática.
- No debe utilizarse software descargado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por el departamento de Sistemas e Informática.
- Para prevenir acciones legales o la adquisición de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita, a menos que haya sido previamente aprobado por el departamento de Sistemas e Informática.
- El personal que utiliza un computador portátil que contenga información confidencial de la empresa, si se va de viaje o se ausenta del cargo, debe hacer entrega al

departamento de Sistemas e Informática del equipo a su cargo para salvaguardar la información.

Esta serie de Políticas descritas anteriormente contribuyen al ordenamiento y administración de los equipos de cómputo y sistemas Informáticos de ARCOPA S.A., por lo tanto es responsabilidad de todos los jefes de áreas aplicar y velar por el cumplimiento de cada uno de estas disposiciones, además reportar a Gerencia General y al departamento de Sistemas e Informática sobre el incumplimiento de estas.

5. Plan de seguridad en las TIC

En esta fase se realizará la verificación del Plan de Seguridad de las tecnologías e información de la empresa, ya que estas deben estar protegidas de posibles riesgos, por ello es necesario aplicar estrategias para reducir dichos riesgos, incorporando adecuadas políticas, procedimientos como también herramientas informáticas especializadas, para que la información cumpla con los criterios de confidencialidad, integridad y disponibilidad; en función de:

- Definir políticas en seguridad de las TIC.

- Políticas para proteger los bienes institucionales, referente al manejo hardware, software e infraestructura tecnológica.
- Políticas de control hacia las operaciones que realizan los usuarios almacenando toda la información necesaria que se efectúa en la organización.
- Desarrollar y hacer uso de normas y procedimientos para la instalación y la actualización periódica de productos antivirus.

- Establecer y mantener actualizadas las políticas y procedimientos para el respaldo y recuperación de la información, que permitan tener acceso a la misma durante periodos de contingencias, causados por desperfectos en los equipos, pérdida de información u otras situaciones similares.

- Evaluar cada uno de los riesgos a los que se exponen las tecnologías de información y comunicación.
- Análisis de control, seguridad, confidencial y respaldos.
- Implementar objetivos de control para evitar, reducir y eliminar riesgos de seguridad que han sido identificados.

Finalmente, es importante señalar las políticas en las TIC, que constituyen una garantía para la seguridad de la empresa:

- El acceso a los sistemas de información, deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información, con acceso que debe controlarse por un administrador y ser manipulado por software.
- Se deben comprobar las responsabilidades de delegación a consultar y/o modificar la información, tomando las medidas de seguridad pertinentes.
- Los datos de los sistemas de información, deben ser respaldados de acuerdo a la frecuencia de actualización de sus datos, con dispositivos de respaldo históricos periódicamente.
- En cuanto a la información de los equipos de cómputo personales, la Unidad de Informática recomienda a los usuarios que realicen sus propios respaldos en la red o en medios de almacenamiento alternos.

- Todos los sistemas de información que se tengan en operación, deben contar con sus respectivos manuales actualizados.
- Implantar rutinas periódicas de auditoría a la integridad, confiabilidad de datos y programas de cómputo.
- Debe realizarse mínimo cada 2 años una evaluación periódica, en el desempeño y gestión de las herramientas de seguridad informática, y de ser necesario, cambiar las soluciones por aquellas que generen mayores características y niveles de seguridad.
- Está restringido acceder o revisar correo que tenga procedencia de remitentes desconocidos, para prevenir los delitos informáticos en el robo de la información, como también las claves de accesos, deben ser cambiados por lo menos 1 vez cada 4 meses, para mayor seguridad de la información.
- Se considera una falta grave, que los usuarios o funcionarios instalen cualquier tipo de programas (software) en sus computadoras, o cualquier equipo conectado a la red de la Municipalidad, que no esté autorizado.
- Ante cualquier cambio en los roles y responsabilidades de los respectivos usuarios de la empresa, deberán ser notificados a la oficina se Sistemas e informática para realizar la respectiva administración de la Red, para el cambio de privilegios.
- El área de informática, tendrá la obligación de realizar acciones en verificación del cumplimiento del Manual de Políticas de Seguridad Informática.

6. Revisión de los niveles de seguridad

- Referenciando los aspectos fundamentales de seguridad, para obtener el impacto de cada activo en las TIC, por ello el marco de trabajo de buenas prácticas de COBIT nos permitirá reducir incidencias de orden natural, física y lógica de la empresa, se basará en un, como lo menciona Osorio (48), ya que permite monitorear el control, la seguridad de TI y evaluar el nivel de madurez en la que se encuentra la empresa, por lo tanto se tendrá en cuenta lo siguiente:

- Seguridad Lógica: Dirigir políticas de seguridad para llevar el control en el acceso a cada uno de los sistemas de información, en redes y sistemas operativos.

- Los sistemas de información en operación, deberán contar con sus respectivos manuales; con los procedimientos de operación y el manual técnico de estructura interna, programas, catálogos y archivos.

- Verificar la información que proceda de fuentes externas a fin de garantizar que esté libre de cualquier agente contaminante o dañina para el funcionamiento de los equipos.

- Proteger los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.

- Seguridad Física: Realizar la respectiva revisión de las instalaciones físicas (cableados), equipamiento tecnológico, áreas de trabajo, a vista de riesgos de seguridad.

- Seguridad Personal: Generar procedimientos de seguridad, permitiendo reducir riesgos que están ligados a los errores humanos, robo (datos, equipos tecnológicos), fraudes, entre otros vinculados al riesgo de las TIC.

7. Programación de Políticas de seguridad:

- Existencia de inventarios periódicos asociados a las TIC.
- Elaborar un plan de mantenimiento de rutina periódico del equipo tecnológico de la empresa, ya que el manejo de estas es constante.
- Evaluación de la seguridad física y de redes.
- Mantener bajo resguardo las licencias de uso de software.
- Verificar si existen garantías para proteger la integridad de los recursos informáticos.
- Verificar si el hardware y software se adquieren siempre y cuando tengan la seguridad de que los sistemas computarizados proporcionaran mayores beneficios que cualquier otra alternativa.
- Análisis de las claves de acceso, control, seguridad, confiabilidad y respaldos.
- Realizar medidas de control interno, seguridad y auditabilidad durante las configuraciones que se realicen en el software.
- Identificar que los procesos de compra de equipos tecnológicos, deben estar sustentados en políticas,

procedimientos y reglamentos, asegurando que todo el proceso se realiza en un marco de legalidad.

- Facilitar la existencia de uno o varios software que gestionen la salida hacia internet y desde internet, filtrado de contenidos, filtrado de páginas y monitoreo de navegación.
- El software de detección de virus deben ser instalado en todos los servidores y equipos de cómputo.
- Tener el mayor control de los usuarios de forma rigurosa de que no se debe conectar a ningún tipo de equipo de comunicaciones con por ejemplo un módem, la cual posibilite la conexión a la Red Corporativa.
- Adquirir políticas de seguridad que regulen el uso y el acceso del servicio de Internet.
- Realizar un informe de auditoría para verificar y dar a conocer las medidas aplicadas ante las amenazas definidas, para que todas las inseguridades y errores que se producen de manera rutinaria disminuyan.
- Comunicar a todo el personal involucrado en el manejo de las TIC, sobre el desarrollo de las políticas.
- Es responsabilidad del área de informática que todos los equipos asignados estén libres de virus, información gestionada y asegurada de la empresa.

8. Administración de operaciones y comunicaciones de TIC

Verificar cada una de las medidas de administración hacia las operaciones y comunicaciones de las TIC, para llevar un mejor control en cada uno de sus procesos y objetivos de la organización, entre estos aspectos se tiene lo siguiente:

- Generar y documentar observaciones hacia los diferentes cambios que se realizan en los ambientes operativos de las tecnologías.
- Realizar controles preventivos y detectar virus, el uso de software de dudosa procedencia, y otros similares.
- Dar a conocer la seguridad sobre los correos electrónicos al recibir informaciones de intrusos informáticos, tratando de infiltrarse y robar información valiosa de la empresa.
- Salvaguardar la seguridad sobre las redes, medios de almacenamiento y documentación de los sistemas de información.
- Mantener un ambiente para medidas adecuadas en prevención de la divulgación de datos sensibles y de desarrollo.
- Implantar planes de contingencia, factible donde detallen acciones, procedimientos, recursos humanos, financieros y tecnológicos que supongan riesgos que afectan de forma improcedente en la operatividad de los servicios de TIC de la empresa.

9. Explorar las actividades periódicas de las TIC

Se tendrán en cuenta las siguientes actividades:

Elaborar un plan de tratamiento de riesgo en implementar controles de seguridad, utilizando un marco de trabajo COBIT de buenas prácticas, generando lo siguiente:

- Evaluar alternativas para el tratamiento de riesgos.
- Efectuar análisis de riesgos, identificando escenas de amenazas.
- Detección de incidentes y eventos de seguridad.

- Implementar acciones correctivas y preventivas.
- Entrenamiento del manejo de la auditoría en seguridad de las TIC.
- Establecer y determinar el método que se utilizará para identificar la seguridad de las actividades seleccionas, especificando los pasos de cómo se utilizarán las medidas de control.
- Descubrimiento de incidentes y eventos de seguridad, dando entender procesos y procedimientos respectivos para actuar rápidamente ante esas incidencias.
- Ejecución de las revisiones periódicas de las TIC, logrando desarrollar procedimientos que aseguren de manera periódica, el monitoreo y manejo adecuado de las TIC y verificar la efectividad de los controles establecidos.

10. Mantener y mejorar la capacitación del personal en el manejo de las TIC

Establecer mecanismos que permitan generar una adecuada capacitación al personal involucrado en los procesos de las TIC, para obtener resultados satisfactorios, minimizando riesgos, alcanzando metas y proyectos establecidos dentro de la empresa, efectuando acciones correctivas y preventivas, ya que es de importancia que los usuarios tengan presente las herramientas y metodologías en la correcta dirección de las TIC. A continuación observaremos acciones importantes a aplicar:

- Realizar capacitaciones periódicas inicialmente en el ambiente de trabajo, esto permitirá que el nuevo usuario llegue a ser instruido con el manual de procedimientos.

- También instruir al usuario suplente, en caso de que el trabajador por cuestiones personales esté ausente en su área.
- Facilitar manuales efectivos de usuarios, de operación y materiales de entrenamiento para aplicaciones y soluciones técnicas, transmitiendo el conocimiento necesario para la operación exitosa de las tecnologías.
- Una estrategia importante que se debe realizar ante nuevos cambios (configuraciones en sistemas) y políticas, es enviar oficios múltiples convocando reuniones de capacitación antes nuevas opciones en los sistemas.
- El área de informática deberá instaurar directivas o reglamentos en materias tecnológicas, siendo de mucha importancia dentro de la empresa, para que cada usuario tome el respectivo conocimiento de sus responsabilidades.

11. Redacción de la auditoría en seguridad de las TIC

- La fase primordial de esta actividad es llegar a realizar la redacción del Manual de Seguridad de TIC, teniendo en cuenta los requerimientos de las auditorías informáticas llevando a cabo el cumplimiento de la Metodología de marco de trabajo de COBIT (53).
- Se deben tener los respectivos procedimientos documentados, y haber generado en la cultura de la organización el hábito de que, antes un no cumplimiento de requerimientos (no conformidad), se generen acciones correctivas.
- La eficiencia, eficacia y calidad de las auditorías que se realizan en las organizaciones se verán favorecidas por la capacitación adecuada del personal y la consecuente automatización de procedimientos.

- Posterior a la lectura del informe previo de Auditoría de resultados, se analizan y se elabora el Informe de Auditoría que contiene los resultados finales de la auditoría que no fuesen superados. El informe de Auditoría debe tener un formato uniforme y está dividido por secciones para facilitar una rápida comprensión del contenido del informe, obteniendo la siguiente información que definida la planificación de controles de análisis de riesgos.
- Observaciones mejoradas, pendientes de efectuar y no implementadas.
- Porcentajes generales de las observaciones implementadas.
- Término del proceso de seguimiento.

4.5.2. Propuesta Económica

El valor del coste a realizar una Auditoría basada en COBIT 4.1, debe suponer como un coste más entre todos los que son necesarios para desempeñar las acciones correctivas de la empresa, como también un grado de garantía de que dicho servicio en aumento con mayor eficacia de los procesos de la empresa.

En el presente se describirán todos los materiales necesarios para realizar la Auditoría basada en COBIT 4.1, para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A., para luego obtener el presupuesto total, como también el tiempo de duración de esta.

Duración: El proyecto tendrá una duración de 250 horas y un aproximado de 2 meses, dejando archivado y documentado todos os procesos de control a seguir. Los integrantes del equipo de Auditoría estarán compuesto por los siguientes:

- **1 Auditor**

Perfil

- Graduado de licenciatura o maestría en seguridad informática o ingeniería de sistemas.
- Experiencia aproximado 2 años de auditar.
- Disciplina
- Orden
- Ser muy meticuloso con todo, incluso con los pequeños detalles.

Habilidades

- Expresarse con claridad tanto en forma oral como escrita.
- Tener necesario una mente crítica que le permita analizar y cuestionar, con sumo cuidado, las diferentes actividades que evalúa.
- Debe sumar a esto un conocimiento amplio, que le permita ofrecer una asesoría constructiva.

Conocimientos

- Conocimientos sobre manteniendo físico y lógico de TIC.
- Conocimientos generales sobre técnicas de análisis, diseño e implantación de sistemas, bases de datos, hardware y telecomunicaciones.
- Conocimientos de conceptos tradicionales de planeación, organización, dirección y control.
- Conocimientos profundos en administración

- **1 Especialista – Analista**

  Perfil

  - Egresado y graduado de licenciatura en informática o ingeniería de sistemas.
  - Experiencia aproximado 2 años.
  - Disciplina
  - Orden

  Habilidades

  - Capacidad de síntesis
  - Capacidad comunicativa
  - Buena oratoria
  - Ser muy meticuloso con todo, incluso con los pequeños detalles.
  - Capacidad de abstracción
  - Capacidad de conceptualizar Conocimientos

  Conocimientos

  - Conocimientos en tecnologías y sistemas de información.
  - Experiencia y dominio de la programación informática.
  - Conocimientos en lenguajes de programación.
  - Capacidad para resolver problemas.

- **1 Asistente**

  Perfil

  - Técnico en el área de informática.

- Experiencia aproximado 1 año.

Habilidades

- Establecer relaciones interpersonales.
- Organizar el trabajo.
- Disciplina
- Iniciativa.
- Expresión y comunicación efectiva tanto oral como escrita.

Conocimientos

- Operación de sistemas de información y tecnologías.
- Manejo de herramientas de productividad.

Tabla Nro.1: Presupuesto de ejecución de Auditoría

Presupuesto y estimación indicada para la realización de la Auditoría	
Categoría de inversión	**Cantidad (S/)**
Costos directos	1,050.00
Capacitaciones de usuarios.	2,050.00
Ejecución de Auditoría	3,500.00
TOTAL	**6,500.00**

Fuente: Elaboración Propia

V. CONCLUSIONES

Según los resultados obtenidos en esta investigación para lograr la implementación de una auditoría basada en COBIT 4.1, para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A., se ha demostrado que hay una gran necesidad y suma urgencia de minimizar riesgos, haciendo uso de técnicas y estrategias de análisis, evaluar controles para el buen uso de las tecnologías de información, por lo tanto se ha concluido que la hipótesis general queda aceptada, ya que los trabajadores encuestados asumen la gran importancia de implementar una Auditoría para elevar el nivel de uso y seguridad de las tecnologías en la empresa. De esta forma, se concluye lo siguiente:

1. Respecto a la Tabla N° 17 se aprecia que el 61.11% de los trabajadores encuestados concluyeron que Si están satisfactoriamente de acuerdo que al implementar la Auditoría será de gran beneficio para un pleno control en cada uno de los procesos de seguridad para la eficiencia, eficacia, confiabilidad de las TIC, logrando la incrementación en el nivel de seguridad de los procesos de TIC de la Empresa ARCOPA S.A.

2. En lo concerniente a la Tabla N° 28 se observa que el 69% de los trabajadores encuestados determinaron que a través de la Auditoría se garantizará un alto nivel de madurez acerca del conocimiento en las operaciones de trabajo de las TIC en la Empresa, la cual será de gran beneficio llegar a una alta capacitación al personal involucrado en TIC sobre la seguridad informática.

3. Finalmente en lo que respecta a la Tabla N° 39 se considera que el 75.19% de los trabajadores encuestados concluyeron que sí están de acuerdo con el desarrollo de una Auditoría para lograr el cumplimiento de análisis, evaluación y control interno de las operaciones de trabajo de las TIC de la Empresa.

VI. RECOMENDACIONES

1. Para mejorar la relación entre el uso de las TIC y el buen desempeño laboral del personal que interactúan con las tecnologías, es de beneficio que la empresa realice y aplique una buena práctica de Auditoría, teniendo instrucciones en marcos de referencia tales como COBIT, que admita en fortalecer cada uno de los procesos ejecutados en la empresa, para alcanzar diariamente evaluaciones de riesgos con el objetivo de minimizar los mismos, identificando procesos de mejora.

2. Es provechoso que el área de TIC llegue a alcanzar la implementación de prácticas y entrenamientos, para el uso correcto de las Tecnologías de Información y Comunicación, con la intención de obtener, conservar y producir esfuerzos laborales logrando una efectividad en el desempeño de trabajo de las TIC.

3. Es conveniente que la empresa investigada elaboré y defina reglamentos que reconozcan la importancia de un adecuado trabajo de las Tecnologías de Información y comunicación, para lograr el monitoreo y la evaluación del marco de trabajo interno de la empresa, para las medir las mejoras de cada uno de los procesos ejecutados en la misma.

4. Se propone mantener el compromiso de mejorar la seguridad de las tecnologías de información y comunicación, ejecutando auditorías, con la finalidad de lograr que todos los procedimientos se estandaricen y se documenten, para llegar a aplicar una guía e investigaciones para futuras mejoras en TIC, que se realicen con respecto al mismo dominio y al mismo rubro de servicio, con el fin de evaluar periódicamente el avance de cada uno de los procesos estudiados en este trabajo.

REFERENCIAS BIBLIOGRÁFICAS

1. Romero MdR, Salao MV. Evaluación y auditoría de Sistemas tecnológicos. , Sistemas; 2014.
2. Plasencia Latour J. "Nivel de gestión de la adquisición e implementación de las tecnologías de información y comunicación (TIC) en la Municipalidad Distrital de Santa, provincia Del Santa, departamento de Ancash en el año 2013". Trabajo de Investigación. Chimbote : Universidad Católica Los Ángeles de Chimbote, Departamento de Ciencias; 2013.
3. O. V. MV. Modelo de Madurez de la Gestión de la Seguridad Informática en el contexto de las Organizaciones Inteligentes. Caracas:, Departamento de Informática; 2009.
4. Santos Llanos , DE. Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de TI, basado en Cobit 5. ; 2016.
5. Alva R. Las Tecnologías de información y comunicación como. Tesis. Lima: Universidad Nacional Mayor de San Marcos, Lima, Perú; 2011.
6. Vera E. Competencia en tecnologías de información y comunicación en docentes del área de comunicación de Instituciones Educativas. Tesis de Posgrado. Callao, Perú:, Lima; 2010.
7. Choque R. Estudio en aulas de innovación pedagógica y desarrollo de capacidades TIC. Tesis doctoral. San Juan de Lurigancho, Lima, Perú.:; 2009.
8. López JA, Zuluaga Tamayo AF. Metodología para el Control de Riesgos para la Auditoría de Bases de Datos. título para optar título de Ingeniero en Sistemas Computacionales. Ecuador: Universidad Tecnológica de Pereira, Departamento de ingenierías; 2013.
9. Arenas Cruz M. GestioPolis. [Online].; 2015 [cited 2018 Abril 20. Available from: https://www.gestiopolis.com/conceptos-generales-de-auditoria/.
10. Auditoría de Sistemas de Información. España:; 2015.
11. Chiavenato I. Introducción a la Teoría General de la Administación. Séptima Edición ed. ed. México: Tlalnepantla, Edo. de México: McGrawHill; 2007.
12. Duarte C. Auditoría de Gestión Empresarial. Primera ed.; 2012.

13. CRAYCE. Compañia de RRHH AYCE. wordpress. [Online].; 2017 [cited 2017 Octubre 20. Available from: https://crayce.wordpress.com/2017/03/22/todo-sobre-la-auditoria-ventajas-desventajas-y-tipo-de-auditoria-informatica-con-su-aplicacion/.
14. Canaves. © Monografias.com S.A. [Online]. [cited 2017 Diciembre 10. Available from: https://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml.
15. Jeremías. "Auditoria de Gestión a las Tecnologías de Información y Comunicaciones". Investigación de OLACEFs. El Salvador, C.A. : CORTE DE CUENTAS DE LA REPÚBLICA; 2011.
16. Cuellar Triana , Pinilla Castañeda. El papel del Auditor frente a una auditoria sobre TIC. Colombia: Universidad de la Salle Bogotá-; 2010.
17. Institute, I. G. Cobit 4.1. [Online].; 2012 [cited 2018 Enero 21. Available from: www.itgi.org.
18. Institute ©2IG. COBIT 4.1. Cuarta ed. Alexander Zapata Lenis CCCATPI, editor. EE.UU; 2007.
19. Paredes EA. Metodología para la auditoría integral de la gestión de las tecnologías de la información. 1st ed. Lima, Perú: Fondo Editorial; 2011.
20. RÍOS H. ITIL v3. Manual íntegro. ; 2005.
21. ITIL® Foundation - Gestión de servicios de TIC. [Online]. [cited 2017 Noviembre 20. Available from: http://faquinones.com/gestiondeserviciosit/itilv3/estrategia_servicios_TI/introduccion_objetivos_activos_servicio.php.
22. Oltra Badenes RF. ITIL® (Information Technology Infrastructure Library). Valencia: Universidad Politécnica de Valencia, Departamento de Organización de Empresas; 2011.
23. Conceptos básicos para la certificación en ITIL®. Trabajo de investigación. Mexico: Universidad Tec Virtual del Sistema Tecnológico de Monterrey ; 2012.
24. El Mapa General de ITIL v.3. Tecnologías con clase mundial.
25. Gustavo Sain. ¿Qué es la seguridad informática? Pensamiento Penal. 2018; V(5).

26. Gómez Vieites. Enciclopedia de la seguridad informática. Seis ed.: Grupo Editorial RA-MA; 2011.
27. Barzana Guesesi. Introducción a la Seguridad Informática. Trabajo infórmativo. España:, UMU.
28. ARCOPA S.A. ARCOPA S.A. [Online].; 2015 [cited 2018 Febrero 12. Available from: www.arcopa.com.pe.
29. Cabero J. Impacto de las nuevas tecnologías de la información y la comunicación en las organizaciones. Grupo. Granada:; 1998.
30. Marquez Graells , Pérez. Impacto de las TIC en Educación. España.:, Departamento de Psicología; 2003.
31. Comisión de las Comunidades Europeas. Tecnologías de la información y de la comunicación en el ámbito del desarrollo. Bruselas:, Departamento de Comunicación de la Comisión al Consejo y al Parlamento Europeo.; 2001.
32. González Soto AP, Gisberte M, Guillem A, Jiménez B, Lladó F, Ralló R. Las nuevas tecnologías en la educación. México: EDUTEC; 1966.
33. Cabero Almenara J. Organizar los recursos tecnológicos. México. :, Centros de recursos.; 1996.
34. Canseco FH. technology for Your Job". En "Technology Buyer's Guide". Fortune, Invierno p. 7F:; 1997.
35. Salazar Barriga O. Glosario de términos sobre administración pública.. UNMSM; 2003.
36. ServiciosTIC.com. [Online].; 2015 [cited 2015 Mayo 27. Available from: http://www.serviciostic.com/las-tic/las-tic-en-las-empresas.html.
37. J. M. [blogspot.com]. [Online]. España; 2015 [cited 2015 Mayo 27. Available from: http://peremarques.pangea.org/tic.htm.
38. Restrepo Rivas L. Las Tecnologías de la Información y las Comunicaciones en la Empresa. Medellín - Colombia:; 1999.
39. Aranguiz , Cabello N, Riquelme E, Rivas K, Rodriguez J, Silva R. Importancia de las TICs en la Auditoría. Trabajo de Investigación. Santiago: Universidad Central Empresa y Sociedad del Conocimiento; 2010.

40. Romero LA. Seguridad Informática. Conceptos generales. Universidad de Salamanca.
41. [Online]. [cited 2015 Marzo 27. Available from: http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml.
42. Nacipucha. Gestión de incidentes y problemas en el área de sistemas con metodología ITIL, para mejorar la utilización de los recursos de la organización. Tesis - Ingeniero en Sistemas Informáticos. Cuenca-Ecuador: Universidad Tecnológica Israel, Departamento de Sistemas Informáticos; 2011.
43. Hernández García C. Metodología ITIL. México: Universidad Iberoamericana Campus; 2009.
44. Seguinfo. wordpress.com. [Online].; 2016 [cited 2016 Abril 16. Available from: https://seguinfo.wordpress.com/2008/12/03/%C2%BFque-es-itil-2/.
45. Cervantes López D, RIvera Trujillo LR, Vallecillo Gómez JL. Bliblioteca de Infraestructura de Tecnologías de Información. Trabajo de Investigación. ; 2013.
46. ISACA: Serving IT Governance Professionals. COBIT. USA:; 2006.
47. ITSOR. Aplicación de metodología de COBIT 4.1. Trabajo de Investigación. , Departamento de Contabilidad; 2009.
48. Glenda Osorio. COBIT. Tacna: UNJBG, Departamento de Ciencias Contables y Financieras.
49. Marin Vergara BE. COBIT. Trabajo de investigación. Tacna:; 2010.
50. ETEK. Corporación multinacional de Seguridad de la Información.
51. Puig J, Blanco S. COBIT. , Departamento de ciencias; 2009.
52. ISACA. COBIT 4.1 en Español. IT Governance Institute; 2007.
53. Institute, IT Governance. COBIT 4.1. Segunda ed. Governance BBoI, editor. Rolling Meadows, IL 60008 EE.UU.: Governance of IT Investments; 2007.
54. Institute. CddCyeIG. COBIT 4.1.: s.l.: Systems Audit and Control Foundation (ISACF); 2007.
55. Guanajuato L. informes@cntec.mx. [Online].; 2016 [cited 2016 Abril 16. Available from: http://cntec.mx/noticias/41-cat-ultimasnoticias/122-

itilvscobit.html.

56. Cervantes Rodriguez. BITCompany. [Online].; 2016 [cited 2016 abril 16. Available from: http://www.bitcompany.biz/diferencia-itil-y-cobit/#.Vx1B6eI6KLc.
57. Directrices de auditoria. Segunda ed.: Information Systems Audit and Control Foundation; 1998.
58. Institute CddCyeIG. Directrices gerenciales. Tercera ed.: s.l. : Information Systems Audit and Control Foundation (ISACF); 2000.
59. Garfinkel. Seguridad Informática: Conceptos básicos.. Informe de investigación. , Acervos Digitales UDLAP; 1999.
60. Alvarez Basaldúa LD. Seguridad en Informática (Auditoría de Sistemas). Tesis para obtener el grado de Maestro en Ingeniería de Sistemas Empresariales. México, D. F. : Universidad Iberoamericana; 1981.
61. Briones G. Metodología de la Invetigacion Cuantitativa en las Ciencias Sociales. Modulo tres ed. Bogotá,Colombia: ARFO Editores e Impresores Ltda; 1996.
62. Galileo Galilei. ; 1564-1642.
63. Bavaresco de Pietro AM. Proceso Metodológico de la Investigación (Como hacer un Diseño de Investigación). Edit. de la Universidad del Zulia. Venezuela: Universidad del Zulia; 1997.
64. Narvaez VPD. Metodologia de la Investigacion Cientifica y Bioestadistica:Para medicos , odontologos y estudiantes de ciencia de la Salud. Segunda ed. Santiago de Chile: RIL editores; 2009.
65. Niño Rojas VM. Metodología de la Investigación: diseño y ejecución. Primera edición ed. Valencia: Ediciones de la U; 2011.
66. Habana UdL. Metodología de la Investigación. En: Selección de Guías de Estudio: Tronco común. Primera edición ed. Madrid: Editorial Universitaria; 2011.
67. Mina Paz Á. Guía práctica de investigación. Primera edición ed. Valencia: El Cid Editor | apuntes; 2009.
68. F. A. Introducción a la Metodología Cientifica. Proyecto de Investigación.

Caracas:; 1999. Report No.: 5th ed..

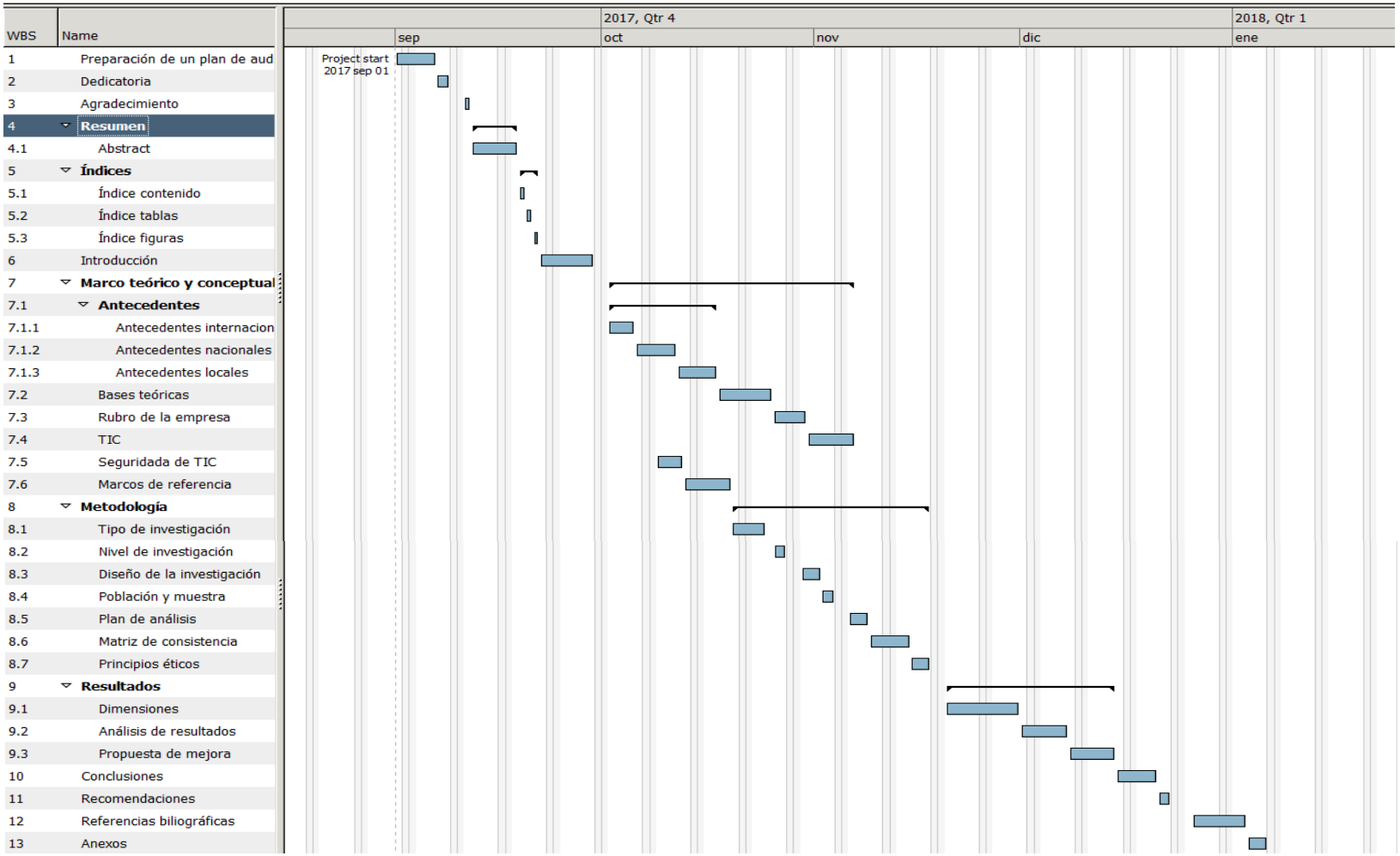
69. ISACA. COBIT® 5. Quinta ed. Rolling Meadows, IL 60008 EE.UU.: ISACA®; 2012.
70. Miranda Domínguez. Nomas ISO 17799. Tema de Investigación. Honduras: Universidad Tecnológica de Honduras, San Pedro Sula; 2012.
71. Asociación Española para la Calidad (AEC). . [Online].; 2017 [cited 2018 Febrero 18. Available from: https://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion.
72. INDECOPI. [Online].; 2017 [cited 2018 Febrero 18. Available from: https://www.indecopi.gob.pe/principios-de-la-seguridad-de-la-informacion.
73. Tarazona T CH. ISO/IEC 17799: Código de práctica para la gestión de la seguridad de la información. Trabajo Informativo. ; 2005.
74. Gómez Fernández L, Andrés Álvarez. Guía de aplicación de la Norma UNE-ISO/IEC 27001. Segunda ed. Gómez Fernández L, Andrés Álvarez A, editors. España: © AENOR (Asociación Española de Normalización y Certificación); 2012.
75. Alcántara Flores JC. Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P en la ciudad de Chiclayo. Tesis Pregrado. Chiclayo: Universidad Católica Santo Toribio de Mogrovejo, Departamento de Ingeniería; 2015.
76. ISOTools Excellence. Blog especializado en Sistemas de Gestión de Seguridad de la Información. [Online].; 2017 [cited 2018 Febrero 25. Available from: https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/.
77. Ortiz Ez. Así se Investiga Pasos para hacer una Investigación. ; 2000. Report No.: ISBN 84-89899-30-4.
78. Chunga F. Diagnóstico y propuesta de mejora del nivel de gestión de la planificación y organización de las tecnologías de información y comunicación en la Municipalidad Distrital de Santa, provincia del Santa, Ancash en el año 2012. [Tesis para optar el título de Ingeniero de sistemas]. Ancash: Universidad

Católica Los Ángeles de Chimbote; 2012.

79. Espinoza P.. Nivel de Seguridad de la Información y Conocimiento de las Tecnologías de Información y Comunicaciones (TICs) en las Municipalidades Distritales de la Provincia de Sullana en el año 2008. [Tesis para optar el título de Ingeniero de sistemas]. Piura- Sullana: Universidad Católica Los Ángeles de Chimbote; 2008.
80. M. A. Nivel de madurez del servicio,configuración,entrenamiento de usuarios,administración de problemas y administración de operaciones,definir y administrar los niveles de servicio de las TIC en la Municipalidad Distrital de Pacaipampa-Ayabaca en el año 2010. [Tesis para optar el título de ingeniero de sistemas]. Piura: Universidad Católica los Ángeles de Chimbote; 2010.

ANEXOS

Anexo N° 1: Cronograma de actividades



Fuente: Elaboración propia

1.1. Anexo N° 2: Presupuesto

Proyecto **:** Escuela de Ingeniería de Sistemas

Título **:** "Auditoría basada en COBIT 4.1, para el uso óptimo de Las TIC y la seguridad informática en la Empresa ARCOPA S.A.; 2017"**.**

Localidad **:** Paita – Piura

Ejecutor **:** Pangalima Albán Ruth Aracelly.

Financiamiento **:** Recursos Propios.

RUBRO	CANT.	COSTO TOTAL
MATERIALES		S/. 63.50
Lapicero	06	S/. 6.00
Papel Bond A4	Millar	S/. 40.00
Resaltador	02	S/. 2.00
Grapas	Caja	S/. 2.00
Folder Manila	02	S/. 8.00
Cuaderno	Unidad	S/. 5.00
SERVICIOS		S/. 110.00
Impresiones	Hoja	S/. 50.00
Copias	Hoja	S/. 30.00
Internet	Hora	S/. 30.00
MOVILIDAD		S/. 580.00
Pasajes	Días	S/.580.00
TOTAL-PRESUPUESTO		**S/. 753.50**

Fuente: Elaboración propia

1.2. Anexo N° 3

ENCUESTA PARA REALIZAR LA PROPUESTA DE UNA AUDITORÍA BASADA EN COBIT 4.1, PARA EL USO ÓPTIMO DE LAS TIC Y LA SEGURIDAD INFORMÁTICA EN LA EMPRESA ARCOPA S.A.

INSTRUCCIONES:

Para realizar la solución de la presente encuesta, tendrá que seleccionar una opción marcando con una X como lo indica la flecha en la opción que corresponde a su respuesta.

Recuerde que los resultados de esta evaluación servirán para alcanzar los coeficientes de validez de contenido del presente cuestionario, agradeciendo de antemano su cooperación.

Ejemplo:

1° **¿**Tiene Usted los conocimientos fundamentales y específicos de los procedimientos del uso de la información y equipamiento para el desarrollo de la organización**?**

SI	NO
X	

1.3. Anexo Nº 4: Cuestionarios

Cuestionario Dimensión N° 01:

N°	Nivel de madurez de los procesos de seguridad para la eficiencia, eficacia, confiabilidad de las Tecnologías de Información y Comunicación.	SI	NO
1°	¿El área de informática cuenta con un manual de organización y funciones?		
2°	¿Se tienen identificados los archivos con información confidencial y se cuenta con claves de acceso?		
3°	¿Se tienen establecidos procedimientos de actualización para estas copias?		
4°	¿Se tiene definido algún proceso para monitorear, evaluar y administrar el recurso humano de TI?		
5°	¿Se registra el acceso al centro de datos de personas ajenas al área de cómputo?		
6°	¿Existen medidas preventivas y correctivas de planes tácticos existentes en la empresa?		
7°	¿Existe un control estricto de las copias de estos archivos?		
8°	¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado?		
9°	¿Se ha realizado una planificación estratégica del sistema de información para la Empresa?		
10°	¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo?		

Cuestionario Dimensión N° 02:

N°	**Nivel de madurez en los grados de conocimiento acerca de los niveles de las operaciones de trabajo de las Tecnologías de Información y Comunicación.**	**SI**	**NO**
1°	¿Se da algún tipo de inducción al personal para que este informado de las funciones que realizará?		
2°	¿Conoces el reglamento implementado dentro del centro de cómputo		
3°	¿Cumples con los reglamentos y políticas estipuladas dentro del centro de cómputo?		
4°	¿El personal de la Unidad de TI posee las competencias y habilidades adecuadas para realizar su función?		
5°	¿Se recibe retroalimentación de la Administración acerca del cumplimiento del plan de trabajo de la Unidad de TI?		
6°	¿Se tiene información del nivel de satisfacción del usuario respecto a los servicios brindados?		
7°	¿Se ha establecido un mecanismo para la atención de incidentes de seguridad de la información?		
8°	¿Se aplican mecanismos para garantizar la protección de los equipos informáticos?		
9°	¿Se cuenta con reglamento para el usuario y personal?		
10°	¿Permiten los niveles actuales que se tenga una ágil de toma de decisiones y comunicación ascendente y descendente?		

Cuestionario Dimensión N° 03:

N°	Nivel de madurez en los grados de evaluación de las operaciones de trabajo de las TIC	SI	NO
1°	¿El área de informática evalúa cada una de las operaciones que se ejecutan dentro de la empresa?		
2°	¿El área de informática cuenta con un plan de seguridad contra perdida de datos?		
3°	¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?		
4°	¿Existe un informe técnico en el que se justifique la adquisición del equipo, software y servicios de computación, incluyendo un estudio costo-beneficio?		
5°	¿Existen políticas establecidas sobre el mantenimiento de los equipos?		
6°	¿El área de informática cuenta con un manual del usuario por sistema?		
7°	¿El área de informática cuenta con procedimientos específicos que indiquen al operador qué hacer cuando un programa interrumpe su ejecución u otras dificultades en proceso?		
8°	¿Se tienen procedimientos que permitan la reconstrucción de un archivo en cinta o disco, el cual fue inadvertidamente destruido?		
9°	¿Están definidas formalmente las funciones y responsabilidades de la Unidad de TI?		
10°	¿Se deja evidencia formal del plan de trabajo, los cambios realizados y la supervisión ejercida?		

1.4. Validación de Instrumentos

UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE
ESCUELA DE POSGRADO

FICHA DE VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1. Nombres y apellidos del validador : Persi Williansh Cabrera Antón
1.2. Cargo e Institución donde labora : Docente - Universidad Nacional de Piura
1.3. Nombre del instrumento evaluado : Cuestionario COBIT
1.4. Autor del instrumento : Ruth Pangalima Albán.

II. ASPECTOS DE VALIDACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (X), según calificación que asigne a cada uno de los indicadores.

1. Deficiente (Si menos del 30% de los ítems cumplen con el indicador)
2. Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador)
3. Buena (Si más del 70% de los ítems cumplen con el indicador)

Aspectos de validación del instrumento		1	2	3	Observaciones Sugerencias
Criterios	Indicadores	D	R	B	
PERTINENCIA	Los ítems miden lo previsto en los objetivos de la investigación.			X	
COHERENCIA	Los ítems responden a lo que se debe medir en la variable y sus dimensiones.			X	
CONGRUENCIA	Los ítems son congruentes entre sí y con el concepto que mide.			X	
SUFICIENCIA	Los ítems son suficientes en cantidad para medir la variable.		X		
OBJETIVIDAD	Los ítems se expresan en comportamientos y acciones observables			X	
CONSISTENCIA	Los ítems se han formulado en concordancia a los fundamentos teóricos de la variable.			X	
ORGANIZACIÓN	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores.			X	
CLARIDAD	Los ítems están redactados en un lenguaje entendible para los sujetos a evaluar			X	
FORMATO	Los ítems están escritos respetando aspectos técnicos (Tamaño de letra, espacio, interlineado, nitidez)		X		
ESTRUCTURA	El instrumento cuenta con instrucciones, consignas, opciones de respuestas bien definidas.			X	
CONTEO TOTAL		0	4	24	
Realizar el conteo de acuerdo a puntuaciones asignadas a cada indicador		C	B	A	TOTAL

Coeficiente de validez: $\frac{A+B+C}{30} = 0.93$

Intervalos	Resultado
0.00 – 0.49	Validez nula
0.50 – 0.59	Validez muy baja
0.60 – 0.69	Validez baja
0.70 – 0.79	Validez aceptable
0.80 – 0.89	Validez buena
0.90 – 100	Validez muy buena

III. CALIFICACIÒN GLOBAL

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado.

VALIDEZ BUENA

Piura, Agosto de 2018

MG. Persi W. Cabrera Antón

UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE
ESCUELA DE POSGRADO

FICHA DE VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1. Nombres y apellidos del validador : Danny Daniel Autan Aanya
1.2. Cargo e Institución donde labora : Docente Uladech Piura
1.3. Nombre del instrumento evaluado : Ruth Pangalima Albain
1.4. Autor del instrumento : Cuestionario COBIT

II. ASPECTOS DE VALIDACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (X), según calificación que asigne a cada uno de los indicadores.

1. Deficiente (Si menos del 30% de los ítems cumplen con el indicador)
2. Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador)
3. Buena (Si más del 70% de los ítems cumplen con el indicador)

Aspectos de validación del instrumento		1	2	3	Observaciones
Criterios	Indicadores	D	R	B	Sugerencias
PERTINENCIA	Los ítems miden lo previsto en los objetivos de la investigación.			X	
COHERENCIA	Los ítems responden a lo que se debe medir en la variable y sus dimensiones.			X	
CONGRUENCIA	Los ítems son congruentes entre sí y con el concepto que mide.			X	
SUFICIENCIA	Los ítems son suficientes en cantidad para medir la variable.		X		
OBJETIVIDAD	Los ítems se expresan en comportamientos y acciones observables			X	
CONSISTENCIA	Los ítems se han formulado en concordancia a los fundamentos teóricos de la variable.			X	
ORGANIZACIÓN	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores.			X	
CLARIDAD	Los ítems están redactados en un lenguaje entendible para los sujetos a evaluar			X	
FORMATO	Los ítems están escritos respetando aspectos técnicos (Tamaño de letra, espacio, interlineado, nitidez)		X		
ESTRUCTURA	El instrumento cuenta con instrucciones, consignas, opciones de respuestas bien definidas.			X	
CONTEO TOTAL		0	4	24	
Realizar el conteo de acuerdo a puntuaciones asignadas a cada indicador		C	B	A	TOTAL

Coeficiente de validez $\frac{A + B + C}{30}$ = 0.93

Intervalos	Resultado
0.00 – 0.49	Validez nula
0.50 – 0.59	Validez muy baja
0.60 – 0.69	Validez baja
0.70 – 0.79	Validez aceptable
0.80 – 0.89	Validez buena
0.90 – 100	Validez muy buena

III. CALIFICACIÒN GLOBAL

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado.

Validez Muy Buena

Piura, Agosto de 2018

Mg. Danny Autan Aanya

UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE
ESCUELA DE POSGRADO

FICHA DE VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1. Nombres y apellidos del validador : Mario Enrique Nizama Reyes
1.2. Cargo e Institución donde labora : Uladech - Piura
1.3. Nombre del instrumento evaluado : Cuestionario COBIT
1.4. Autor del instrumento : Ruth Pangelina Albán

II. ASPECTOS DE VALIDACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (X), según calificación que asigne a cada uno de los indicadores.

1. Deficiente (Si menos del 30% de los ítems cumplen con el indicador)
2. Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador)
3. Buena (Si más del 70% de los ítems cumplen con el indicador)

Aspectos de validación del instrumento		1	2	3	Observaciones
Criterios	Indicadores	D	R	B	Sugerencias
PERTINENCIA	Los ítems miden lo previsto en los objetivos de la investigación.			X	
COHERENCIA	Los ítems responden a lo que se debe medir en la variable y sus dimensiones.			X	
CONGRUENCIA	Los ítems son congruentes entre sí y con el concepto que mide.			X	
SUFICIENCIA	Los ítems son suficientes en cantidad para medir la variable.		X		
OBJETIVIDAD	Los ítems se expresan en comportamientos y acciones observables			X	
CONSISTENCIA	Los ítems se han formulado en concordancia a los fundamentos teóricos de la variable.			X	
ORGANIZACIÓN	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores.			X	
CLARIDAD	Los ítems están redactados en un lenguaje entendible para los sujetos a evaluar			X	
FORMATO	Los ítems están escritos respetando aspectos técnicos (Tamaño de letra, espacio, interlineado, nitidez)		X		
ESTRUCTURA	El instrumento cuenta con instrucciones, consignas, opciones de respuestas bien definidas.			X	
CONTEO TOTAL		0	4	24	
Realizar el conteo de acuerdo a puntuaciones asignadas a cada indicador		C	B	A	TOTAL

Coeficiente de validez $\frac{A + B + C}{30} = 0.93$

Intervalos	Resultado
0.00 – 0.49	Validez nula
0.50 – 0.59	Validez muy baja
0.60 – 0.69	Validez baja
0.70 – 0.79	Validez aceptable
0.80 – 0.89	Validez buena
0.90 – 100	Validez muy buena

Mg. M-Nizama

III. CALIFICACIÒN GLOBAL

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado.

Validez Muy buena

Piura, Agosto de 2018