UNIVERSIDAD NACIONAL
"SANTIAGO ANTUNEZ DE MAYOLO"

ESCUELA DE POSTGRADO

APLICACIÓN DE LA METODOLOGÍA COBIT 5 PARA LA MEJORA DE PROCESOS DE AUDITORIA Y SEGURIDAD INFORMÁTICA EN LA EMPRESA DATCO S&H, HUARAZ

Tesis para optar el grado de maestro
en Ciencias e Ingeniería

Mención en Auditoría y Seguridad Informática

EMERSON ELÍ CHAVEZ ANGELES

Asesor: **Dr. EDDY JESÚS MONTAÑEZ MUÑOZ**

Huaraz – Ancash - Perú

2020

N°. Registro: T0727.

FORMATO DE AUTORIZACIÓN PARA PUBLICACIÓN DE TESIS Y TRABAJOS DE INVESTIGACIÓN, PARA A OPTAR GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES EN EL

REPOSITORIO INSTITUCIONAL DIGITAL - UNASAM

Conforme al Reglamento del Repositorio Nacional de Trabajos de Investigación – RENATI.
Resolución del Consejo Directivo de SUNEDU Nº 033-2016-SUNEDU/CD

1. Datos del Autor:

Apellidos y Nombres: **Chávez Angeles Emerson Elí**
Código de alumno: **2013.2525.9.AI** Teléfono: **943691469**
Correo electrónico: **emerson_dat@hotmail.com** DNI o Extranjería: **31673752**

2. Modalidad de trabajo de investigación:

☐ Trabajo de investigación ☐ Trabajo Académico
☐ Trabajo de suficiencia profesional ☒ Tesis

3. Título profesional o grado académico:

☐ Bachiller ☐ Título ☐ Segunda especialidad
☐ Licenciado ☒ Magister ☐ Doctor

4. Título del trabajo de investigación:

APLICACIÓN DE LA METODOLOGÍA COBIT 5 PARA LA MEJORA DE PROCESOS DE AUDITORIA Y SEGURIDAD INFORMÁTICA EN LA EMPRESA DATCO S&H.

5. Facultad de:.....

6. Escuela, Carrera o Programa: **Maestría en Ciencias e Ingeniería con Mención en Auditoria y Seguridad informática**

7. Asesor:

Apellidos y Nombres: **Montañez Muñoz Eddy** Teléfono: **943517125**
Correo electrónico: **eddyjesus@yahoo.com** DNI o Extranjería: **17834352**

A través de este medio autorizo a la Universidad Nacional Santiago Antúnez de Mayolo, publicar el trabajo de investigación en formato digital en el Repositorio Institucional Digital, Repositorio Nacional Digital de Acceso Libre (ALICIA) y el Registro Nacional de Trabajos de Investigación (RENATI).

Asimismo, por la presente dejo constancia que los documentos entregados a la UNASAM, versión impresa y digital, son las versiones finales del trabajo sustentado y aprobado por el jurado y son de autoría del suscrito en estricto respeto de la legislación en materia de propiedad intelectual.

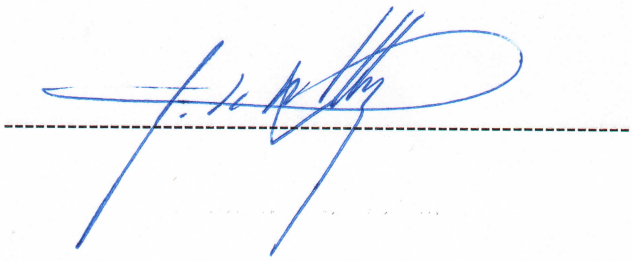
Firma: .....

D.N.I.: 31673752

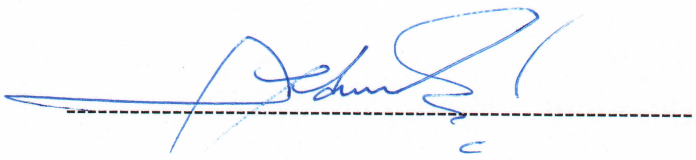
FECHA: 25 / 02 / 2020

MIEMBROS DEL JURADO

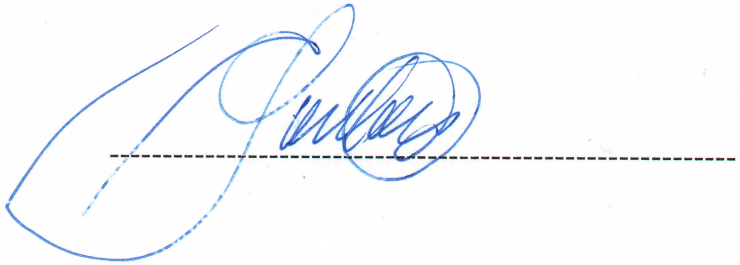
Magister Cesar Augusto Narro Cachay — Presidente



Magister Alberto Martín Medina Villacorta — Secretario



Doctor Eddy Jesús Montañez Muñoz — Vocal



ASESOR

Doctor Eddy Jesús Montañez Muñoz.

AGRADECIMIENTO

- Un agradecimiento singular debo a mi asesor Dr. Eddy Montañez Muñoz que, me ha orientado, apoyado y corregido con un interés y una entrega que han sobrepasado, con mucho, todas mis expectativas que deposité en su persona.

- Al Sr. Godwin Chávez Ángeles, Gerente General de la Empresa DATCO S&H por darme su tiempo y las facilidades para realizar la presente tesis.

A Dios siempre me protege y me guía,

A mis Padres Juan Chávez y Lucila Ángeles, por su ayuda incondicional,

A mis hijos Hugh y Yasira, por cambiar mi vida y darme cada día felicidad.

INDICE

Página

RESUMEN

Las organizaciones usan las tecnologías de información y comunicación (TICs) para facilitar la gestión y control de sus procesos internos, fijando como directriz principal la alineación con las estrategias empresariales establecidas. Partiendo de esta premisa, se fija como objetivo general del presente trabajo presentar los resultados de la aplicación de la norma COBIT 5 en el proceso de transferencias de datos contables, financieros y administrativos del área de Gerencia General de la Empresa DATCO S&H. La organización considera que dicho proceso es crítico, lo cual se justifica gracias al valor de la información transferida en la elaboración de informes de gestión. Se trata de un proyecto factible, el cual involucra la aplicación de conocimiento, a través del uso de un modelo o marco de trabajo relacionado con la administración de recursos informáticos.

Palabras clave: Auditoria informática, COBIT, transferencia de datos, procesos.

ABSTRACT

The organizations use information and communication technologies to facilitate the management and control of its internal processes, setting as the main guideline established alignment with business strategies. On this premise, secured overall objective of this paper to present the results of applying the COBIT 5 standard in the process of transferring accounting, financial and administrative data area General Manager of the Company DATCO S&H. The organization believes that this process is critical, which is justified because the value of the information transferred in the preparation of management reports. This is a feasible project, which involves the application of knowledge through the use of a model or framework relating to the management of computer resources.

Key words: IT Audit, COBIT, data transfer processes.

I. INTRODUCCION

En el marco del plan de modernización de DATCO S&H, dentro del ámbito de la administración y desarrollo de las labores propias, la Gerencia General busca establecer una metodología estandarizada para abordar las distintas áreas en cuanto a la seguridad de la información.

La diversidad de estándares internacionales para la gestión de las tecnologías de información ha aumentado en los últimos años, siendo el COBIT el estándar internacional más completo, el cual incluye objetivos de control específicos considerando el ciclo de calidad de Deming (Plan, Do, Check, Act), para los diversos aspectos relacionados a la gestión de las tecnologías de información: gestión de procesos relacionados con la infraestructura de tecnología de información, gestión de proyectos de infraestructura de tecnología de información, gestión de proyectos de desarrollo de sistemas de información, y gestión de requerimientos relacionados a los sistemas de información en producción; organizados en los grandes temas: Planificación y Organización; Adquisición e Implementación; Entrega de Servicios y Soporte; y Monitoreo y Control. Sin embargo, pese a su existencia, no se dispone de procedimientos específicos dentro del marco de una metodología para el desarrollo de auditorías de la gestión de tecnologías de información, aunque existen algunos procedimientos aislados que han propuesto algunas organizaciones como ISACA, orientados principalmente a la auditoría de aspectos técnicos. Además, en la gestión de tecnologías de información comúnmente se cometen muchos errores que en su conjunto estarían impidiendo o retrasando el logro de los objetivos

organizacionales con los consecuentes perjuicios en las organizaciones usuarias de las tecnologías de información, de todo sector económico y tamaño. Por ello se hace necesario mejorar el proceso de evaluación de la gestión informática en los diversos tipos de organizaciones, siendo este el primer paso para que se pueda realizar una planificación estratégica de tecnología de información integrada a las demás funciones de la organización.

La presente tesis contribuye a la solución de este problema a través de una propuesta metodológica alineada a los estándares internacionales más importantes para la auditoría de la gestión de las tecnologías de información, mejorándose el proceso general de la auditoria, enlazándolo e integrándolo con estándares internacionales (COBIT, ISO/IEC 12207, ISO/IEC 27002, ISO/IEC 20000 y PMBOK) de manera que se logren evaluaciones integrales mucho más acertadas y se contribuya al logro de los objetivos organizacionales. Esta metodología propuesta fue aprobada en dos de las empresas de seguros más importantes del Perú y ya ha sido validada y corregida, siendo un aporte importante para mejorar la gestión informática en las organizaciones peruanas.

Planteamiento y formulación del Problema

Las organizaciones emprenden grandes inversiones en tecnología de información, muchas veces sin evaluar el impacto que realmente tienen en la generación de valor de las mismas. Existen diversas normas dictadas por organismos supervisores como la Contraloría General de la república y la Superintendencia de Banca, Seguros y AFP, así como diversos estándares de calidad que han sido propuestos por diversas entidades a nivel mundial. Estas normas si bien nos ilustran de manera amplia, técnica y ordenada sobre los elementos a tener en cuenta para una adecuada gestión informática, no nos orientan de manera específica sobre los procedimientos a seguir para una evaluación integral de la gestión informática orientada al logro de los objetivos de un Plan Estratégico Organizacional (que se miden sobre la base de indicadores de gestión y resultados a alcanzar establecidos para toda la organización), lo que sería el primer paso a seguir, si queremos lograr una planificación estratégica de la tecnología de información, orientada hacia el logro de los objetivos organizacionales.

La presente tesis pretende cubrir este vacío de conocimiento proponiendo una metodología para la Mejora de procesos de TI, que permita enlazar los diversos conceptos propuestos por los más importantes estándares de calidad internacionales, y de esa manera, permita contribuir a la generación de valor de las organizaciones que la utilicen.

Por ello concluimos en el siguiente enunciado de problema:

¿En qué medida se mejorará la Auditoría y Seguridad Informática en la empresa DATCO S&H con la aplicación de la metodología COBIT 5?

Objetivos

Objetivo General

Implementar la metodología COBIT 5 para mejorar los procesos de auditoria y seguridad informática en la empresa DATCO S&H.

Objetivos específicos

1. Identificar si hay diferencia en los procesos de auditoria y seguridad informática, dimensión gestión de riesgos, antes y después de la implementación de la metodología COBIT 5.
2. Identificar si hay diferencia en los procesos de auditoria y seguridad informática, dimensión seguridad informática, antes y después de la implementación de la metodología COBIT 5.
3. Definir y construir las Metas de Cascada de COBIT 5

Hipótesis

Con la implementación de la metodología COBIT 5 se mejora los procesos de auditoria y seguridad informática en la empresa DATCO S&H.

Esto se demostrará, si: hay diferencias estadísticamente significativas en los procesos de auditoria y seguridad informática, antes y después de la implementación de la metodología COBIT 5

Variables

Según la hipótesis encontramos dos variables, una independiente V.I y la otra dependiente V.D. Como describimos a continuación:

V.I. Metodología COBIT 5

V.D. Procesos de Auditoria y seguridad informática

En anexo, se presenta la matriz de operacionalización de variables, en el que se detallan las dimensiones, se identifican los indicadores y se asocian los ítems del instrumento de toma de datos, en la columna valoración se muestran los valores iniciales para los indicadores, los que serán cuantificados en su dimensión real con la toma de datos en campo.

Justificación

- ✓ Justificación Tecnológica:

  Los recursos tecnológicos a utilizar están basados en software libre, estando a alcance de la empresa DATCO S&H.

- ✓ Justificación Económica:

  Es un proyecto desarrollado con presupuesto del investigador y no generarán gastos para la empresa DATCO S&H

- ✓ Justificación Operativa:

  Facilitar la aplicación de COBIT 5 para la mejora de procesos de auditoria y seguridad informática en la empresa DATCO S&H.

- ✓ Justificación Social:

  Al tratarse de un proyecto que busca optimizar el proceso de auditoría y seguridad informática, se alcanzará una mejoría en el desempeño y la productividad reflejándose en la satisfacción del personal.

- ✓ Justificación Legal:

  Por tratarse de un Empresa Constructora, que presta servicios a empresas privadas y públicas, se debe verificar el cumplimiento de la normatividad y leyes emitidas por las autoridades correspondientes.

Delimitación

- ✓ **Geográficas.** Este proyecto se desarrollará en la Empresa DATCO S&H ubicado en la Av. Palmira N° 139 Urbanización Santa Elena Independencia – Huaraz – Ancash.
- ✓ **Temporales.** El proyecto de investigación se llevará a cabo en un lapso de 1 año desarrollando cada objetivo propuesto, a partir de la aprobación del anteproyecto.
- ✓ **Conceptuales.** Los conceptos que abarcan esta investigación van relacionados con gobierno corporativo de TI.

II. MARCO TEORICO

2.1. Antecedentes

En el marco de las investigaciones realizadas hasta la fecha, en el campo de la Construcción y su mezcla con la metodología COBIT 5, existen un número reducido de investigaciones, citamos los trabajos de:

- En Perú-Trujillo Universidad Nacional de Trujillo (2016), "Modelo de evaluación del proceso de mantenimiento de sistemas de información de la C.A.C. Chiclayo LTDA. Basado en COBIT 5".

- En Perú-Lima Universidad Peruana de Ciencias Aplicadas UPC (2015), "Implementación de un modelo de gestión estratégico de TI para la empresa IT-Expert"

- En Perú-Huancayo Universidad Nacional del Centro del Perú (2014), "Aplicación de COBIT para mejorar el nivel de gestión de las tecnologías de la información y la comunicación en la red de salud valle del Mantaro"

- En Ecuador Sangolqui (2012), "Auditoria de Riesgos informáticos del departamento de sistemas de Caves SAEMA utilizando COBIT como marco de Referencia" por Aucancela Soliz, Jorge Geovanni, Obtuvo como resultados La administración del riesgo tecnológico debido a que involucra el uso de recursos organizaciones, humanos, financieros y tecnológicos.

- En Colombia, Santiago de Cali (2012), “Caracterización de Procesos de Gestión de TI basados en COBIT 5, para la implementación en la industria Editorial Colombiana” por Muñoz Serna Rodrigo, Martínez Arias Mario Alberto, Obtuvo como resultados Una caracterización y mapeo de procesos de Gestión de TI basados en COBIT 5, como guía referente de implementación en la industria editorial Colombiana. Tomando como insumo la guía de procesos habilitadores de COBIT 5 se construye la caracterización de procesos de gestión de TI COBIT 5, relacionando la descripción del proceso, metas de TI, Indicadores de TI, luego por cada proceso sus prácticas con su descripción, responsable y actividades de cada práctica.

- En México (2009), “Metodología para el establecimiento de objetivos de control como un medio de seguridad en el Área de Tecnologías de Información” por Prado Oseguera Diana Marisol, se Obtuvo como resultado Mitigar los riesgos del Área de TI.

2.2. Bases Teóricas

2.2.1. Metodología COBIT 5

COBIT 5 proporciona la guía de nueva generación de ISACA para el gobierno y la gestión de las TI en la empresa. Se construye sobre más de 15 años de uso práctico y aplicación de COBIT por parte de

muchas empresas y usuarios de las comunidades de negocio, TI, riesgo, seguridad y aseguramiento.

La publicación COBIT 5 contiene el marco COBIT 5 para el gobierno y la gestión de las TI de la empresa.

El marco COBIT 5 se construye sobre cinco principios básicos, que quedan cubiertos en detalle e incluyen una guía exhaustiva sobre los catalizadores para el gobierno y la gestión de las TI de la empresa.

La familia de productos de COBIT 5 incluye los siguientes productos:

- COBIT 5 (el marco de trabajo)
- Guías de catalizadores de COBIT 5, en las que se discuten en detalle los catalizadores para el gobierno y gestión, estas incluyen:
  - COBIT 5: Información Catalizadora
  - Información posibilitadora (en desarrollo)
  - Otras guías de catalizadores (visitar www.isaca.org/cobit)
- Guías profesionales de COBIT 5, incluyendo:
  - Implementación de COBIT 5
  - COBIT 5 para Seguridad de la Información (en desarrollo)
  - COBIT 5 para Aseguramiento (en desarrollo)
  - COBIT 5 para Riesgos (en desarrollo)
  - Otras guías profesionales (visitar www.isaca.org/cobit)

- Un entorno colaborativo online, que estará disponible para dar soporte al uso de COBIT 5

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a **crear el valor óptimo** desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público.

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.

2.2.2. Procesos de auditoria

La auditoría puede definirse como un proceso sistemático por el cual un equipo o una persona competente e independiente obtienen y evalúan objetivamente la evidencia respecto a las afirmaciones acerca de un proceso con el fin de formarse una opinión sobre el particular e informar sobre el grado de cumplimiento en dicha afirmación que es implementada.

Una auditoría puede ser realizada por una o varias personas debidamente capacitadas cuya visión debe ser clara y objetiva respecto a lo que se va a inspeccionar, de aquí que surja el entredicho de que no todas las personas pueden o deben ser auditores ya que esto conlleva un examen personal, para poder emitir opiniones constructivas que ayuden a la entidad a mejorar sus procesos.

Finalmente, con base en la experiencia del equipo de trabajo, definimos el concepto de Auditar como el estudio de los mecanismos de control que están implementados en una organización identificando si estos son adecuados y cumplen con los objetivos y estrategias de la entidad, estableciendo los cambios que se deben realizar para la consecución de los mismos.

La **auditoría informática** es el proceso de recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información

salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos. Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

Los objetivos de la auditoria informática son:

- ✓ El control de la función informática
- ✓ El análisis de la eficiencia de los Sistemas Informáticos
- ✓ La verificación del cumplimiento de la Normativa en este ámbito
- ✓ La revisión de la eficaz gestión de los recursos informáticos
- ✓ La auditoría informática sirve para mejorar ciertas características en la empresa como:
  - Eficiencia
  - Eficacia
  - Rentabilidad
  - Seguridad

2.2.3. Seguridad Informática

Hoy en día son múltiples los riesgos asociados a que equipos y sistemas de información y comunicaciones no cuenten con controles de seguridad. Las amenazas en las TIC son globales, y están repartidas en distintos niveles de criticidad según sea la orientación y el ámbito de su utilización. Preocupante es para grandes, medianas y pequeñas organizaciones el espionaje industrial, los ladrones de información, la interrupción de servicios y las fallas críticas en la infraestructura y sistemas centrales de información.

Cada día, se desarrollan nuevos métodos que afectan a la seguridad de la información de las organizaciones, es por ello la necesidad de una estrategia completa de seguridad, de manera de prevenir fugas y fallas en los sistemas. A lo antes expuesto se suman vulnerabilidades internas (misma organización), que son un factor de riesgo no menor, y por lo tanto, existe alta probabilidad de pérdida de dinero y repercusiones en la confiabilidad por parte de usuarios, clientes y socios de negocios.

No se pueden obviar los factores de riesgos por desastres que al no estar previstos eficientemente y sin planes de contingencia y/o de recuperación pueden provocar daños irreparables en tiempo y costos de recuperación. Esto, que es difícilmente cuantificable, puede incluso determinar la continuidad de una organización.

Se puede entender como seguridad cualquier tipo de estado que el sistema está libre de riesgo, daño o peligro. Entendiendo por riesgo, daño o peligro aquellos aspectos que pueden afectar el funcionamiento directo o los resultados que se obtienen del mismo. Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

- **Integridad**.- La información sólo puede ser modificada por quien está autorizado y de manera controlada.
- **Confidencialidad**.- La información sólo es legible para los usuarios que están autorizados.
- **Disponibilidad**.- La información debe de estar disponible cuando se necesita.
- **No Repudio**, Irrefutabilidad, irrenunciabilidad.- El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

2.3. Definición de Términos

Actividad (ISACA, 2012)

En COBIT, la acción principal tomada para operar el proceso. Directrices para alcanzar prácticas de gestión para un gobierno y gestión de TI exitoso en la empresa. Actividades:

- Describe un conjunto de tareas orientadas a la acción necesarios y suficientes para alcanzar una Práctica de Gobierno o una Práctica de Gestión.

- Considerar las entradas y salidas del proceso.
- Se basan en estándares y buenas prácticas aceptados de forma generalizada.
- Apoyan el establecimiento de roles y responsabilidades claros.
- No son prescriptivos y deben adaptarse y desarrollarse en procedimientos apropiados para la empresa.

Alineamiento (ISACA, 2012)

Un estado en el que los elementos facilitadores del gobierno y la gestión de TI de la empresa contribuyen a las metas y las estrategias de la misma.

Aplicación TI (ISACA, 2012)

Funcionalidad electrónica que constituye una parte de los procesos de negocio que se realizan por o mediante la ayuda de TI.

Arquitectura de aplicación (ISACA, 2012)

Descripción de las capacidades de agrupación lógica de las capacidades de gestión de los objetos necesarios para procesar la información y contribuir a las metas corporativas.

Atributo (de capacidad) de un proceso (ISACA, 2012)

ISO/IEC 15504: Una característica medible de una capacidad de proceso aplicable a cualquier proceso.

Autenticación

El acto de verificar la identidad de un usuario y sus derechos de acceso a información en los sistemas.

Buena práctica (ISACA, s.f.)

Una actividad o proceso probado que se ha puesto en práctica con éxito por múltiples empresas y se ha demostrado que produce resultados fiables.

Capacidad de un proceso (ISACA, 2012)

Ser adecuado para un propósito (conseguir el valor deseado)

Catalizador (facilitador)

Factores externos e internos que inician y afectan cómo la empresa o el individuo actúan o cambian.

COBIT (ISACA, 2012)

COBIT 5 conocido antiguamente como Objetivos de Control para Tecnologías de Información o Relacionadas (COBIT); usado actualmente solo como un acrónimo en su quinta revisión. Un marco completo, internacionalmente aceptado, para el gobierno y la gestión de la información de la empresa y la tecnología de la información (TI) que soporta a los ejecutivos de la empresa y los gestores en la definición y consecución de las metas de negocio y las metas de TI relacionadas.

COBIT describe cinco principios y siete facilitadores que dan soporte a las empresas en el desarrollo, implementación y mejora continua y supervisión de buenas prácticas relacionadas con el gobierno y la gestión de TI.

Código de ética (Acha Iturmendi, 1994)

Un documento diseñado para influir en el comportamiento individual y en el organizativo de los empleados al definir los valores organizativos y las reglas que se aplican en ciertas situaciones. Se adopta para ayudar a aquellos que dentro de la organización son llamados a tomar decisiones de forma que puedan entender la diferencia entre decisiones 'correctas' e 'incorrectas' y aplicar esta comprensión a sus decisiones.

Contexto (Del Peso, 2001)

El conjunto completo de factores internos y externos que pueden influir o determinar cómo actúa una empresa, entidad, proceso o individuo.

El contexto incluye:

- Contexto tecnológico – Factores tecnológicos que afectan la capacidad de una organización para extraer valor de los datos
- Contexto de datos – La precisión de los datos, su disponibilidad, grado de actualización y calidad.
- Habilidades y conocimiento – Experiencia general y habilidades analíticas, técnicas y de negocio
- Contexto organizativo y cultural – Factores políticos, y si la organización prefiere datos a la intuición

- Contexto estratégico – Metas corporativas estratégicas

Continuidad de negocio (ISACA, 2012)

Evitar, mitigar y recuperarse de una interrupción. Se puede usar en este contexto también los términos "planificación de la restauración del negocio", "planificación para recuperación de desastres" y "planificación de las contingencias"; se enfocan en los aspectos de la recuperación dentro de la continuidad y, por esa razón, el factor "resiliencia" también debería ser considerado.

Control (ISACA, 2012)

Los medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden tener una naturaleza administrativa, técnica, de gestión, o legal. También usada como sinónimo de salvaguarda o contramedida.

Control de procesos de negocio (ISACA, 2012)

Las políticas, procedimientos, prácticas y estructuras organizativas diseñadas para generar garantías razonables de que un proceso de negocios conseguirá sus objetivos.

Creación de valor (ISACA, 2012)

El objetivo principal del gobierno de una empresa, conseguido cuando los tres objetivos subyacentes (consecución de beneficios, optimización de riesgo y optimización de recursos) están en equilibrio.

Cultura (ISACA, 2012)

Un patrón de comportamientos, creencias, hipótesis, actitudes y formas de hacer las cosas.

Entradas y Salidas (ISACA, 2012)

Los elementos/productos del trabajo en un proceso que se consideran necesarios para soportar la operación de un proceso. Son los que posibilitan la toma de decisiones clave, proveen un registro y traza de auditoría de las actividades del proceso y posibilitan el seguimiento en caso de un incidente. Se definen al nivel de práctica de gestión clave y pueden incluir algunos productos de trabajo usados únicamente dentro del proceso y son, comúnmente, entradas esenciales para otros procesos. Las entradas y salidas de COBIT 5 son ilustrativas y no deben considerarse como una lista exhaustiva ya que se pueden definir flujos de información adicionales dependiendo del entorno particular de una empresa y de su marco de procesos.

Gestión (Heredero, López Hermoso Agius, Romo Romero, & Medina Salgado, 2013)

Incluye el uso juicioso de medios (recursos, personas, procesos, prácticas, etc.) para conseguir un fin identificado. Es un medio o instrumento mediante el cual el grupo que gobierna consigue un resultado u objetivo. La gestión es responsable de la ejecución dentro de la dirección establecida por el grupo que gobierna. La gestión se refiere a las actividades operacionales de planificación, construcción, organización y control que alinean con la dirección que establece el grupo que gobierna y la información sobre dichas actividades.

Marco Contextual

La empresa **DATCO S&H S.R.L.,** es una empresa de Ingeniería, creada en Setiembre de 1996 en base a profesionales de amplia experiencia en la Ingeniería, acotando de esta forma a los retos de las Empresas del presente y a las condiciones del mercado de los servicios de Ingeniería.

DATCO S&H S.R.L., tiene por finalidad prestar servicios de ingeniería en ejecución y asesoría de Obras civiles, eléctricas y sanitarias, Arquitectura, Topografía Digital y Satelital, Hidrología e Hidráulica, Obras Civiles en Minería y Sistemas Informáticos.

Nuestros servicios están destinados a las empresas privadas, empresas de servicio público, organismos multilaterales y gobiernos.

Actualmente, la Empresa sigue aliada con los siguientes socios comerciales, BARRICK, NYRSTAR, JME CONSTRUCTORA, TDM TECNOLOGIA DE MATERIALES, PROSEGUR, GOLDER ASSOCIATES, DUKE ENERGY, ENERSUR, AES CHANGUINOLA, ABENGOA PERU, SN POWER, HIDRANDINA, RIO DOBLE S.A., gracias a este respaldo está en constante desarrollo, involucrando directamente a su capital humano, y tecnológico en el desarrollo de soluciones que persigue.

En la actualidad DATCO S&H tiene implementado diversos sistemas informáticos instalados en su servidor local y conectados a través de redes locales y además periódicamente incrementa la infraestructura de TI. Estos sistemas demandan la adquisición de equipos, adecuación de ambientes, contrato de algunos servicios, capacitación de personal, etc. Luego de una indagación preliminar se ha podido establecer que en general, la gestión de la seguridad de estos activos no se está realizando siguiendo estándares establecidas de seguridad, lo cual pone en riesgo a estos activos y a la información que procesan, lo que podría ocasionar un grave impacto negativo en DATCO S&H. No se está realizando un análisis de riesgos, evaluación de las amenazas, vulnerabilidades ni existen planes de contingencia ante la eventual materialización de una amenaza. Frente a esta situación es necesario tomar acciones de prevención a fin de proteger los activos de información existentes, así como la continuidad de las actividades apoyadas por sistemas informáticos.

A medida que realizaba sus operaciones iba adquiriendo diversa tecnología sin seguir una metodología para la administración correcta, por lo tanto, ahora surgen problemas que retrasan los trabajos en consecuencia pérdida de recursos.

Es necesario entonces determinar con claridad su estructura, para tener los elementos necesarios que permitan identificar el alcance de la auditoria de sistemas.

La estructura orgánica funcional de DATCO S&H se puede observar en la siguiente Figura:

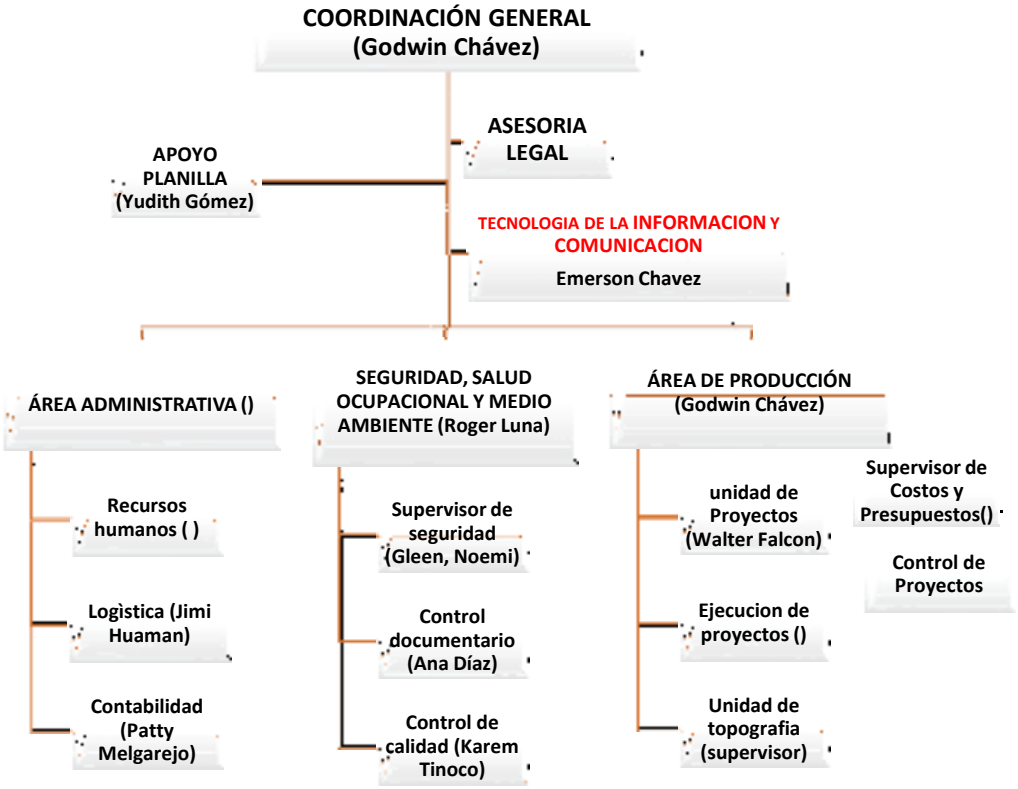


Figura 1: Organigrama de DATCO S&H

DESCRIPCION DE FUNCIONES DEL NIVEL DIRECTIVO

Se considera importante hacer una descripción general de las funciones de quienes trabajan en la empresa especialmente en el nivel ejecutivo de los departamentos con incidencia relevante en el desarrollo de la auditoria de sistemas.

COORDINACIÓN GENERAL

- Ejecutar las políticas, normas y procedimientos de la empresa.
- Dirigir la marcha institucional, coordina y evalúa las actividades técnicas y administrativas de DATCO S&H.
- Cumplir y hacer cumplir los reglamentos, estatutos y demás normas vigentes de la empresa.
- Analizar y aprobar los estados financieros de la empresa.
- Aplicar reglamentos, manuales, procedimientos técnicos y administrativo financieros de la empresa.
- Coordina la ejecución de los programas y/o proyectos, y evaluar su cumplimiento.
- Determinar políticas sobre el desarrollo de la Empresa y la administración de sus recursos.
- Dirigir la planificación estratégica, técnica, económica, financiera y administrativa de DATCO S&H.
- Implementar políticas para el mejoramiento funcional de la empresa.

CARACTERISTICAS DE LOS SISTEMAS Y AMBIENTE COMPUTARIZADO

DATCO S&H tiene sus oficinas en una nueva construcción en la ciudad de Huaraz con instalaciones eléctricas adecuadas.

Estructura de hardware: DATCO S&H posee:

SERVIDOR

CARACTERISTICAS:

Procesador Intel Core 1.4 GHz

Memoria RAM: 8Gb

Número de usuarios: 50

Sistema operativo: Windows server 2008

Espacio total en disco duro: 1Tb

ESTACIONES DE TRABAJO

HP Y COMPATIBLES

Tipo: notebooks y desktops

Memoria RAM: Mínima: 4Gb

Procesador Mínimo: Pentium CORE i3

Tiene una red UTP de categoría 5e con Hubs y Switch a 10 y 100 Mbps.

ESTRUCTURA DE SOFTWARE: DATCO S&H cuenta con el siguiente software:

SISTEMA OPERATIVO EN LAS ESTACIONES:

Windows xp, Windows 7, Windows 8 (idioma: español)

SOFTWARE UTILITARIO

Entre los principales utilitarios utilizados en DATCO S&H podemos mencionar:

- Microsoft Office 2010 Profesional

- Microsoft Project 2010
- PDF Converter Enterprise 8 – Nuance
- Winzip
- Antivirus la empresa cuenta con Panda Gold
- AutoCAD
- S10

Todo el software se encuentra debidamente licenciado.

III. METODOLOGÍA

3.1. Tipo y diseño de Investigación

El presente trabajo de investigación es de Tipo explicativa, pues se establecerá una relación directa entre los activos de información, los riesgos a los cuales éstos están expuestos y la metodología COBIT 5, que nos debe permitir optimizar los procesos y la gestión de riesgos informáticos.

Diseño de Investigación

El diseño de investigación es cuasi experimental longitudinal. Para la recolección de la información se recurrirá a las encuestas con los colaboradores administrativos y gerente general responsables por los activos a estudiar y para facilitar la recolección de datos se usarán formatos y encuestas de acuerdo a los activos a evaluar. La evaluación se hará en dos etapas una antes de la aplicación de la metodología COBIT 5 y otra después de la aplicación de la metodología COBIT 5

3.2. Plan de recolección de la información y/o diseño estadístico

- **Población**

  La población de estudio en esta investigación está definida como todos los responsables de la gestión de activos de información de la administración central de DATCO S&H que son en total 96 colaboradores, y también sistemas informáticos, servidor, redes LAN y otros.

- **Muestra**

20 gestores responsables del control de los activos de información siguientes:

- Sistemas de Información
- Servidores.
- Redes LAN.

Los activos se han elegido por la importancia que representan para DATCO S&H y la muestra ha sido seleccionada con un enfoque no probabilístico pero que involucra al personal que administra directa e indirectamente dichos activos.

N°	GESTOR	AREA
1	Windows 10	Todas las Áreas
2	Servidor	Centro de Datos
3	Red LAN	Todas las Áreas
4	PCs	Todas las Áreas
5	Laptops	Todas las Áreas
6	S10	Área de Producción
7	AutoCAD	Área de Producción
8	Civil 3D	Área de Producción
9	Software Contable	Área Administrativa
10	USBs	Todas las Áreas
11	Disco Duro Red	Centro de Datos
12	Redes Sociales	Todas las Áreas
13	Acceso a datos	Centro de Datos
14	Respaldos	Centro de Datos
15	Confidencialidad	Centro de Datos
16	Disponibilidad	Centro de Datos

17	Integridad	Centro de Datos
18	Antivirus	Todas las Áreas
19	Credenciales	Centro de Datos
20	Base de Datos	Centro de Datos

Unidad de Análisis

La unidad de análisis es un gestor responsable del control de los activos de información antes mencionados con las vulnerabilidades y amenazas que enfrentan, el impacto que tendría en la organización una eventual falla de éste, así como la gestión que se está realizando con cada uno de ellos.

Validación de la investigación

Se hará mediante la comparación en cuanto a tiempo y calidad de resultados, para lo cual se deben comparar los resultados obtenidos por diferentes métodos:

- Aplicación de encuestas para la medición de desempeño de los procesos involucrados con las variables de la investigación en dos momentos: Pre y Post prueba.
- El juicio de Expertos.
- Controles que se desarrollara como parte del presente trabajo.

3.3. Instrumentos de recolección de la información

Encuestas realizadas a los colaboradores de la Empresa DATCO S&H, gestores de los activos informáticos.

3.4. Plan de procesamiento y análisis estadístico de la información

- ✓ Recopilación de la bibliografía relacionada con los estándares de calidad internacionales: COBIT, ISO/IEC 12207, ISO/IEC 27002 (antes 17799), ISO/IEC 20000 Y PMBOK.
- ✓ Elaboración de la metodología para la auditoría integral de la gestión informática.
- ✓ Aplicación de la metodología para la auditoría integral de la gestión informática.
- ✓ Afinamiento de la metodología.
- ✓ Aplicación de la metodología afinada.
- ✓ Evaluación de los resultados. Se evaluó el impacto resultante de la aplicación de la metodología para la auditoría integral de la gestión informática.

Para contrastar la hipótesis se hizo uso de la estadística inferencial, para ello se tuvo en cuenta el análisis de la estadística paramétrica con la prueba T-Student para muestras relacionadas, con un nivel de significación del 5% ($p<0,05$).

IV. RESULTADOS

4.1 Presentación de Resultados

4.1.1. Análisis de la situación actual

Basada en la creciente competencia y complejidad de los negocios y en el permanente desarrollo tecnológico que soporta y crea nuevas oportunidades y desafíos, DATCO S&H ha visto la necesidad de contar con sistemas de información que manejen y automaticen las distintas actividades, tanto claves como de soporte, generando eficiencia y productividad, pero al mismo tiempo estructurando ambientes tecnológicos cada vez más complejos. Aspectos como alta sistematización de los procesos, automatización de los controles, integración de la información, importancia fundamental de la información para la toma de decisiones, exponen a las organizaciones a nuevos riesgos que deben ser adecuadamente administrados y/o gestionados.

La Gerencia general no tiene plan para realizar supervisión lo cual causa:

- Falta de visibilidad
- Estrategia desintegrada
- Mala integración
- Duplicación
- Complejidad
- Altos costos

- Falta de atención
- Fragmentación
- Desperdicio de información
- Desperdicio de recursos.

4.1.2. Diagnóstico de la situación actual

Sin embargo, un buen inicio para aplicar COBIT durante la revisión sería direccionar la gestión de TI en los aspectos relacionados con:

- Falla al atender los requerimientos de los usuarios
- Falla en la integración
- Incompatibilidad con la infraestructura técnica
- Problemas con el soporte del proveedor
- Instalaciones costosas y complejas

Consciente de esta situación, DATCO S&H, ha visto la necesidad de afrontar un proyecto de buenas prácticas, cuyos resultados le permitirán entre otras cosas:

- Promover una cultura de conciencia del riesgo asociado a los sistemas y tecnología de la información.
- Implementar mecanismos de control para una adecuada administración de las actividades de sistemas.
- Implementar políticas y procedimientos que permitan una adecuada administración de las distintas actividades y recursos tecnológicos.

- ❖ Incrementar la calidad del servicio que el Área de Sistemas brinda a los usuarios.
- ❖ Enfocar las actividades hacia los objetivos estratégicos del negocio.
- ❖ Optimizar la utilización de los recursos tecnológicos.
- ❖ Mejorar la gestión de los sistemas informáticos, para obtener información confiable y de calidad.
- ❖ Mejorar la calidad de los servicios tecnológicos proporcionados por terceros.

La auditoría y seguridad informática, por lo tanto, constituye para DATCO S&H en una decisión estratégica, puntualizada como resultado de todo un proceso de análisis, definiciones y pruebas a través de la aplicación del modelo COBIT, marco referencial que nos provee una serie de objetivos de control necesarios para evaluar y reforzar el ambiente de control IT.

4.1.3 Del diseño

De acuerdo a los requerimientos acordados con DATCO S&H, hemos definido la evaluación de las siguientes etapas:

1. **Estructura Organizacional del Área de Sistemas**
   a. Estructura de Personal
   b. Evaluación de Gestión del área
   c. Atención al usuario

2. **Gestión de los Sistemas Informáticos**

   a. Desarrollo, operación y Mantenimiento de Aplicaciones

   b. Administración de las Bases de Datos (DBA)

   c. Gestión y Explotación de las Aplicaciones

3. **Plataforma y Comunicaciones**

   a. Plataforma Tecnológica, Redes y Comunicaciones

4. **Evaluación de Seguridades y Procedimientos de Continuidad**

   a. Seguridades: Físicas, Lógicas y de Comunicaciones

   b. Plan de Contingencias

MÉTODO DE TRABAJO Y PROCEDIMIENTO A EJECUTAR

El enfoque de trabajo considerará las siguientes etapas:

1. **Estructura Organizacional (Controles sobre las actividades IT)**

   En esta etapa las tareas a ejecutar son:

   Análisis de Situación Actual

   - Entrevistas con los funcionarios del área de informática y áreas usuarias destinadas a evaluar el ambiente general de control en materia de tecnología existente.
   - Relevamiento de actividades y procesos (con el alcance mínimo necesario para determinar segregación de funciones).
   - Revisión de los procedimientos de control implantados.
   - Reunión de validación.

Elaboración de mejoras potenciales

- Compilación Basada en estándares de control (COBIT).
- Reuniones de validación y discusión.

Procedimientos Detallados

Se ejecutarán los siguientes procedimientos:

1.1. Estructura de Personal

- Dependencia, roles y responsabilidades del personal del área informática.
- Evaluación de la segregación de funciones.
- Análisis del perfil de cada cargo tipo y sus ocupantes (experiencia, capacitación y estudios).

1.2. Evaluación de la Gestión

- Evaluar los procesos y estándares y probar su cumplimiento.
- Evaluar el proceso de planeamiento y la razonabilidad del plan informático respecto a los objetivos de la organización.
- Evaluar los procedimientos de asignación de recursos y la elaboración y administración de presupuesto, así como la razonabilidad de los recursos asignados.

1.3. Atención al Usuario

- Análisis del procedimiento establecido para asegurar que el servicio sea acorde con las necesidades de los usuarios.

- Evaluación de los procedimientos de atención a usuarios y administración de problemas.

2. Gestión de los Sistemas Informáticos

En esta etapa las tareas a ejecutarse son:

Análisis de Situación Actual

- Relevamiento detallado de la funcionalidad implantada.
- Características generales de las aplicaciones (tablas, reportes).
- Seguridades.

Elaboración de mejores potenciales

- Elaboración de conclusiones y recomendaciones, a partir del material relevado y estándares de control, utilizando herramientas de análisis de riesgos y objetivos de control para cada aplicación.
- Reuniones de validación y discusión.

Procedimientos Detallados

Se ejecutarán los siguientes procedimientos:

2.1. Desarrollo, Operación y Mantenimiento de Aplicaciones

- Revisar y evaluar la metodología de desarrollo de aplicaciones existente.
- Relevar los procedimientos para desarrollo de aplicaciones utilizados.
- Evaluar los procedimientos e iniciativas de investigación y desarrollo.
- Evaluar los procedimientos para pasar los programas de ambiente de desarrollo a producción.

- Revisar la documentación de la planificación de mantenimiento / mejora de aplicaciones, así como la documentación que sustenta la prueba y otros procesos de recepción por parte del usuario.
- Evaluar los procedimientos de operación.
- Revisar las bitácoras de operación.
- Revisar los procedimientos de schedulling y revisar las bitácoras de ejecución de los procesos batch.
- Revisar los procedimientos vigentes para backup de información (tipo de información, periodicidad, lugar de almacenamiento y pruebas periódicas de los respaldos).

2.2. Administración de la Base de Datos (Dba)

- Evaluar los procedimientos de administración de la base de datos.
- Revisar el sistema de documentación de la base de datos (nivel de detalle y actualización de la información).
- Analizar roles y responsabilidades de la administración de la base de datos.

2.3. Gestión y Explotación de las Aplicaciones

- Relevar información relativa a las aplicaciones como:
  - Características generales.
  - Responsables.
  - Plataforma tecnológica.
  - Principales módulos.
  - Mecanismos de seguridad disponibles.
  - Documentación existente.

- Interfaces con otros sistemas.
- Implantaciones en curso.

- Evaluar la seguridad y control de cada aplicación.

3. Plataforma y Comunicaciones

En esta etapa las tareas a ejecutarse son:

Análisis de situación Actual

- Relevamiento detallado de Hardware utilizado en cada aplicación
- Análisis de niveles de servicio (capacidad, velocidad, tiempos de parada).

Elaboración de mejoras potenciales

- Elaboración de conclusiones y recomendaciones, a partir del material relevado y de las prácticas comunes en compañías de tamaño similar y estándares de control COBIT.
- Reuniones de validación y discusión.

Procedimientos Detallados

Se ejecutarán los siguientes procedimientos:

3.1. Plataforma Tecnológica, Redes y Comunicaciones

- Revisión de los procedimientos de medición del rendimiento. Análisis de los informes de rendimiento disponibles.
- Revisión de los procedimientos relativos al monitoreo de la red. Análisis de la bitácora de problemas.

- Análisis de los mecanismos de comunicación y acceso a los datos de la red desde el punto de vista de disponibilidad.
- Relevar las herramientas de monitoreo de hardware y software existentes, y compararlas con las disponibles en el mercado.
- Revisar procedimientos de respaldo (mirroring, líneas de comunicación alternativas).
- Relevamiento de la arquitectura del sistema, incluyendo:
  - Servicios de red implementados.
  - Diagrama de la red.
  - Servidores.
  - Equipos de redes LAN.
  - Cableado estructurado.
  - Enlaces WAN.
  - PC's por ubicación.

4. Evaluación de Seguridades y Procedimientos de Continuidad

En esta etapa las tareas a ejecutarse son:

Análisis de Situación Actual

- Revisión de seguridad de las plataformas utilizando herramientas específicas.
- Evaluación del Plan de Contingencias.

Elaboración de mejores potenciales

Se efectuarán mediante:

- Elaboración de conclusiones y recomendaciones, a partir del material relevado y de las prácticas comunes en compañías de tamaño similar y estándares de control COBIT.
- Reuniones de validación y discusión.

Procedimientos Detallados

Se ejecutarán los siguientes procedimientos:

4.1. Seguridades: Físicas, Lógicas y Comunicaciones

- Evaluar las políticas y procedimientos de seguridad vigentes.
- Revisar la seguridad lógica implantada en los servidores, así como los parámetros de seguridad relativos a las claves de acceso, utilizando la herramienta de software específicas para cada plataforma. Esto comprende, entre otros:
  - Tipo y longitud mínima y máxima de las claves de acceso.
  - Manejo de claves de acceso históricas.
  - Encriptación de claves.
  - Administración de claves de acceso por servicio.
  - Rotación de claves de acceso (automático o manual) y periodicidad.
  - Número de intentos fallidos antes de ingresar al sistema.
  - Número de sesiones simultáneas por usuario.
  - Número de perfiles de usuario.
- Tiempo permitido de inactividad en el sistema (time out).
- Verificar la activación y revisión de logs y pistas de auditoría.

- Revisar las seguridades de accesos remotos (dial up, internet, intranet).
- Evaluar los mecanismos de protección de antivirus,
- Evaluar los mecanismos de seguridad física existentes, incluyendo contratos de seguros existentes,

4.2. Plan de Contingencias

- Evaluar la estrategia de recuperación, infraestructura tecnológica y las facilidades para la continuidad del procesamiento.
- Evaluar los procedimientos de recuperación y operación durante la emergencia, tomando en cuenta: responsables, actualización, pruebas periódicas, metodología para la determinación de los procedimientos.

HERRAMIENTAS A UTILIZAR

Su utilización garantiza que el trabajo sea realizado con los más altos estándares internacionales:

Kali-Linux: Es una herramienta automatizada que permite la revisión de seguridades en redes LAN, computadoras.

4.1.4 DE LA IMPLEMENTACIÓN

IDENTIFICACIÓN DE RIESGOS IT CRÍTICOS

Los procedimientos a ejecutar como parte de la auditoría y seguridad informática se detallan a continuación, con asociación al Dominio y Objetivo de control del modelo COBIT aplicado para la evaluación e identificación de debilidades.

1. ESTRUCTURA ORGANIZACIONAL DEL AREA DE SISTEMA (CONTROLES SOBRE LAS ACTIVIDADES IT)

Se ejecutarán los siguientes procedimientos:

1.1. ESTRUCTURA DE PERSONAL

	COBIT		
Procedimiento	**Dominio**	**Código**	**Objetivo de Control**
Dependencia, roles y responsabilidades del personal del área informática.	Planeación y Organización	PO4	Definición de la Organización y de las Relaciones IT.
Evaluación de la segregación de funciones.	Planeación y Organización	PO4	Definición de la Organización y de las Relaciones IT – Segregación de Funciones (4.10)
Análisis del perfil de cada cargo tipo y sus ocupantes (experiencia, capacitación y estudios).	Planeación y Organización	PO7	Administración de Recursos Humanos

1.2. EVALUACIÓN DE GESTIÓN

	COBIT		
Procedimiento	**Dominio**	**Código**	**Objetivo de Control**
Evaluar los procesos y estándares y probar su cumplimiento.	Planeación y Organización.	PO6	Comunicación de la dirección y aspiraciones de la gerencia – Comunicación de las políticas de la organización (6.3)
Evaluar el proceso de planeamiento y la razonabilidad del plan informático respecto a los objetivos de la organización.	Planeación y Organización.	PO1	Definición de un Plan Estratégico de Tecnología de Información.
Evaluar los procedimientos de asignación de recursos y la elaboración y administración de presupuestos, así como la razonabilidad de los recursos asignados.	Planeación y Organización.	PO10	Administración de proyectos.

1.3. ATENCIÓN AL USUARIO

	COBIT		
Procedimiento	**Dominio**	**Código**	**Objetivo de Control**
Análisis del procedimiento establecido para asegurar que el servicio sea acorde con las necesidades de los usuarios.	Entrega de servicios y soporte.	DS8	Apoyo y asistencia a los Clientes de Tecnología de Información.
Evaluación de los procedimientos de atención a usuarios y administración de problemas.	Entrega de servicios y soporte.	DS10	Administración de problemas e incidentes.

2. GESTIÓN DE LOS SISTEMAS INFORMÁTICOS

Se ejecutarán los siguientes procedimientos:

2.1. DESARROLLO, OPERACIÓN Y MANTENIMIENTO DE APLICACIONES

	COBIT		
Procedimiento	**Dominio**	**Código**	**Objetivo de Control**
Revisar y evaluar la metodología de desarrollo de aplicaciones existente.	Planeación y Organización	PO11	Administración de Calidad – Metodología del Ciclo de Vida de Desarrollo de Sistemas (11.5)
Relevar los procedimientos para desarrollo de aplicaciones utilizados.	Planeación y Organización	PO11	Administración de Calidad
Evaluar los procedimientos e iniciativas de investigación y desarrollo.	Planeación y Organización	PO10	Administración de proyectos
Evaluar los procedimientos para pasar los programas de ambiente de desarrollo a producción.	Adquisición e Implementación	A15	Instalación y Acreditación de Sistemas
Revisar la documentación de la planificación de mantenimiento / mejora de aplicaciones, así como la documentación que sustenta la prueba y otros procesos de recepción por parte del usuario.	Adquisición e Implementación	A12	Adquisición y Mantenimiento de Software de Aplicación
Evaluar los procedimientos de operación	Adquisición e Implementación	A14	Desarrollo y Mantenimiento de Procedimientos relacionados con Tecnología de Información.
Revisar las bitácoras de operación.	Planeación y Organización	A14	Desarrollo y Mantenimiento de Procedimientos relacionados con Tecnología de Información.
Revisar los procedimientos de schedulling y revisar las bitácoras de ejecución de los procesos batch.	Entrega de servicios y Soporte	DS13	Administración de Operaciones
Revisar los procedimientos vigentes para backup de información (tipo de información, periodicidad, lugar de almacenamiento y pruebas periódicas de los respaldos).	Entrega de servicios y Soporte	DS11	Administración de la Información

2.2. ADMINISTRACIÓN DE LAS BASES DE DATOS (DBA)

	COBIT		
Procedimiento	**Dominio**	**Código**	**Objetivo de Control**
Evaluar los procedimientos de administración de la base de datos	Planeación y organización	PO2	Definición de la Arquitectura de Información
Revisar el sistema de documentación de la base de datos (nivel de detalle y actualización de la información)	Planeación y organización	PO2	Definición de la Arquitectura de Información
Analizar roles y responsabilidades de la administración de la base de datos.	Planeación y organización	PO2	Definición de la Arquitectura de Información

2.3. GESTIÓN Y EXPLOTACIÓN DE LAS APLICACIONES

	COBIT		
Procedimiento	**Dominio**	**Código**	**Objetivo de Control**
Relevar información relativa a las aplicaciones como: - Características generales - Responsables - Plataforma tecnológica - Principales módulos - Mecanismos de seguridad disponibles	Adquisición e implementación	A12	Adquisición y Mantenimiento de Software de Aplicación.

- Documentación existente - Interfaces con otros sistemas - Implementaciones en curso			
Evaluar la seguridad y control de cada aplicación	Entrega de Servicios y Soporte	DS5	Garantizar la Seguridad de Sistemas

3. PLATAFORMAS Y COMUNICACIONES

Se ejecutarán los siguientes procedimientos:

3.1. PLATAFORMA TECNOLÓGICA, REDES Y COMUNICACIONES

	COBIT		
Procedimiento	**Dominio**	**Código**	**Objetivo de Control**
Revisión de los procedimientos de medición del rendimiento. Análisis de los informes de rendimiento disponibles.	Entrega de Servicios y Soporte	DS3	Administración de Desempeño y Capacidad
Revisión de los procedimientos relativos al monitoreo de la red. Análisis de la bitácora de problemas.	Entrega de Servicios y Soporte	DS3	Administración de Desempeño y Capacidad
Análisis de los mecanismos de comunicación y acceso a los datos de la red desde el punto de vista de disponibilidad.	Entrega de Servicios y Soporte	DS3	Administración de Desempeño y Capacidad

Relevar las herramientas de monitoreo de hardware y software existentes, y compararlas con las disponibles en el mercado	Entrega de Servicios y Soporte	DS3	Administración de Desempeño y Capacidad
Revisar procedimientos de respaldo (mirroring, líneas de comunicación alternativas)	Entrega de Servicios y Soporte	DS4	Aseguramiento de Servicio Continuo
Relevamiento de la arquitectura del sistema, incluyendo: - Servicios de red implementados - Diagrama de la red - Servidores - Equipos de redes LAN - Cableado estructurado - Enlaces WAN - PC2s por su posición	Entrega de Servicios y Soporte	DS9	Administración de la Configuración

4. EVALUACIÓN DE SEGURIDADES Y PROCEDIMIENTOS DE CONTINUIDAD

Se ejecutarán los siguientes procedimientos:

4.1. SEGURIDADES: FÍSICAS, LÓGICAS Y DE COMUNICACIONES

	COBIT		
Procedimiento	**Dominio**	**Código**	**Objetivo de Control**
Evaluar las políticas y procedimientos de seguridad vigentes.	Entrega de Servicios y Soporte	DS5	Garantizar la Seguridad de Sistemas
Revisar la seguridad lógica implantada en los servidores, así como los parámetros de seguridad relativos a las claves de acceso, utilizando la herramienta de software específicas para cada plataforma. Esto comprende, entre otros: - Tipo y longitud mínima y máxima de las claves de acceso. - Manejo de claves de acceso históricas. - Encriptación de claves. - Administración de claves de acceso por servicio. - Rotación de claves de acceso (automático o manual) y periodicidad. - Número de intentos fallidos antes de ingresar al sistema. - Número de sesiones simultáneas por usuario. - Número de perfiles de usuario.	Entrega de Servicios y Soporte	DS5	Garantizar la Seguridad de Sistemas
Tiempo permitido de inactividad en el sistema (time out)	Entrega de Servicios y Soporte	DS5	Garantizar la Seguridad de Sistemas

Verificar la activación y revisión de logs y pistas de auditoría.	Adquisición e Implementación	A11	Identificación de Soluciones de Automatización – Diseño de Pistas de Auditoría (1.10)
Revisar las seguridades de accesos remotos (dial up, internet, intranet).	Entrega de Servicios y Soporte	DS5	Garantizar la Seguridad de Sistemas
Evaluar los mecanismos de protección de antivirus.	Entrega de Servicios y Soporte	DS5	Garantizar la Seguridad de Sistemas
Evaluar los mecanismos de seguridad física existentes, incluyendo contratos de seguros existentes.	Entrega de Servicios y Soporte	DS12	Administración de Instalaciones

4.2. PLAN DE CONTINGENCIAS

	COBIT		
Procedimiento	**Dominio**	**Código**	**Objetivo de Control**
Evaluar la estrategia de recuperación, infraestructura tecnológica y las facilidades para la continuidad del procesamiento.	Entrega de Servicios y Soporte	DS4	Aseguramiento de Servicio Continuo
Evaluar los procedimientos de recuperación y operación durante la emergencia, tomando en cuenta: responsables, actualización, pruebas periódicas, metodología para la determinación de los procedimientos.	Entrega de Servicios y Soporte	DS4	Aseguramiento de Servicio Continuo

Conforme a lo acordado en la propuesta de trabajo, se procedió en DATCO S&H la Auditoria y seguridad informática relacionada con las Evaluación de los servicios de tecnología de información. En tal virtud se cubrirán los siguientes aspectos:

1. Evaluación de la Estructura Operacional del Área de Sistemas.
2. Evaluación de los Sistemas Informáticos.
3. Evaluación de las Plataformas y Comunicaciones.
4. Evaluación de Seguridades y Procedimientos de Continuidad

Como resultado de la tesis, se detalla los problemas más relevantes que inciden globalmente en la eficacia y eficiencia de los servicios tecnológicos requeridos por DATCO S&H.

- ✓ **Comité de sistemas**

  Estructurar y formalizar las actividades del Comité de Sistemas, el cual deberá ser el encargado de la planificación, supervisión y priorización de las distintas actividades que realiza el Área Tecnológica.

- ✓ **Administración de Seguridades**

  Definir las funciones de Administración de Seguridades independiente del Área de Sistemas, que será responsable del desarrollo, implantación y monitoreo de todas las políticas y procedimientos de seguridad.

- ✓ **Esquema de Seguridades**

  Definir un esquema estándar de seguridades para todas las aplicaciones, así como mejorar las reglas de construcción de claves.

- ✓ **Atención al Usuario**

  Reorganizar el Área de Atención al Usuario, estableciendo un canal de comunicación único, facilitando de esta manera la atención, seguimiento y solución de los requerimientos de los usuarios.

  Asimismo, es necesario establecer una política clara, en donde se detallen las tareas que están asignadas al responsable de atención al usuario (Help Desk) con sus prioridades de solución y herramientas para atención y seguimiento.

- ✓ **Políticas y Procedimientos**

  Desarrollar políticas y procedimientos formales que le permitan a la gerencia controlar y supervisar las distintas actividades del Área de Sistemas.

  Ejemplos:

  - Procedimientos para la ejecución de procesos Batch
  - Procedimientos de Atención al usuario
  - Procedimientos para el monitoreo del rendimiento de los equipos y base de datos.

- ✓ **Recuperación ante interrupciones**

  Elaborar e Implementar procedimientos alternativos de operación durante fallas de tal manera de brindar un mejor y continuo servicio a los clientes, los procedimientos deben estar acordes a la estructura tecnológica, riesgos y servicios de la Empresa.

Además de las siguientes mejoras:

Mejora de eficiencia operativa de la organización: Alineación estratégica, y reducción de costos de operación.

Mejora de percepción de la gestión: Confiabilidad, Transparencia, Disminución de jugas de información

Blindaje, Reducción de riesgos de gestión: Marco operativo formal, Monitoreo continuo con tableros de control dinámicos.

Sistema de gestión de Cumplimiento: Aseguramiento, Atención de auditorías.

Resultados comparables entre el "antes y el después" de aceptación a los entregables de las iniciativas.

Niveles aceptables de incertidumbre para los involucrados.

Proactividad efectiva en la consecución (o descarte) de beneficios.

Consistencia entre las necesidades, las actividades y los resultados de formación; respecto a las competencias necesarias para los involucrados.

4.2 Prueba de Hipótesis

Con respecto al objetivo general (hipótesis planteada)

Paso 1. Hipótesis de Investigación

Con la implementación de la metodología COBIT 5 se mejorarán los procesos de auditoria y seguridad informática en la empresa DATCO S&H.

Paso 2. Hipótesis estadística

H_0: No hay diferencias estadísticamente significativas en los procesos de auditoria y seguridad informática, antes y después de la implementación de la metodología COBIT 5.

H_1: Si hay diferencias estadísticamente significativas en los procesos de auditoria y seguridad informática, antes y después de la implementación de la metodología COBIT 5.

Paso 3. Se determina el nivel de significación: Usando un nivel de significancia del 5% (α=0,05)

Paso 4. Se elige el estadígrafo de prueba: $$t = \frac{\overline{d}}{\sigma_d / \sqrt{n}}$$

Se trabajó con la prueba estadística T-Student, para muestras relacionadas, con un nivel de significación del 5% (p < 0,05).

Paso 5: Prueba para muestras relacionadas

TABLA N° 2: Resultados de las encuestas antes y después de la implementación de la metodología COBIT 5**.**

Puntaje obtenido	**Antes**		**Después**	
	nº	**%**	**nº**	**%**
60 – 70	2			
70 – 80	8			
80 – 90	10			
90 - 100	-		-	
100 – 110	-		15	
110 - 120	-		5	
Total	20	100	20	100
Media	78,90		108,20	
D.e.	6,15		4,62	

Fuente: Encuesta ejecutada por el investigador

PRE Y POST PRUEBA	DIFERENCIAS RELACIONADAS		PRUEBA T PARA IGUALDAD DE MEDIAS		
	Media	Desv. estándar	t	gl	Valor p
GRUPO EXPERIMENTAL	29,30	6,99	18,75	19	**0,00001**

Paso 6. Se determina regla de decisión:

Rechazar la Hipótesis nula si el valor p es menor que 0,05 ($p<0,05$). Para un nivel de confianza de 95%, que equivale a un valor $\alpha = 0,05$ se ha obtenido $T = 18,75$ con un valor $p < 0,05$ por lo que se rechaza la hipótesis nula

Paso 7. Interpretación y/o conclusión:

Como la hipótesis nula ha sido rechazada, se confirma que hay diferencias estadísticamente significativas en los procesos de auditoria y seguridad informática, antes y después de la implementación de la metodología COBIT 5.

Por lo que se concluye que la implementación de la metodología COBIT 5 mejora los procesos de auditoria y seguridad informática de la empresa.

Con respecto al objetivo específico 1

Paso 1. Objetivo específico 1

Identificar si hay diferencia en los procesos de auditoria y seguridad informática, dimensión gestión de riesgos, antes y después de la implementación de la metodología COBIT 5.

Paso 2. Hipótesis estadística

H_0: No hay diferencias estadísticamente significativas en los procesos de auditoria y seguridad informática, dimensión gestión de riesgos, antes y después de la implementación de la metodología COBIT 5.

H_1: Si hay diferencias estadísticamente significativas en los procesos de auditoria y seguridad informática, dimensión gestión de riesgos, antes y después de la implementación de la metodología COBIT 5.

Paso 3. Se determina el nivel de significación: Usando un nivel de significancia del 5% (α=0,05)

Paso 4. Se elige el estadígrafo de prueba: $$t = \frac{\overline{d}}{\sigma_d / \sqrt{n}}$$

Se trabajó con la prueba estadística T-Student, para muestras relacionadas, con un nivel de significación del 5% (p < 0,05).

Paso 5: Prueba para muestras relacionadas

TABLA N° 3: Resultados de las encuestas antes y después de la implementación de la metodología COBIT 5, dimensión gestión de riesgos**.**

Puntaje obtenido	**Antes**		**Después**	
	nº	**%**	**nº**	**%**
30 – 40	2		-	
40 – 50	10		-	
50 – 60	8		-	
60 – 70	-		8	
70 – 80	-		12	
Total	20	100	20	100
Media	48,65		71,90	
D.e.	5,80		3,88	

Fuente: Encuesta ejecutada por el investigador

PRE Y POST PRUEBA	DIFERENCIAS RELACIONADAS		PRUEBA T PARA IGUALDAD DE MEDIAS		
	Media	Desv. estándar	t	gl	Valor p
GRUPO EXPERIMENTAL	23,25	6,56	15,85	19	**0,00001**

Paso 6. Se determina regla de decisión:

Rechazar la Hipótesis nula si el valor p es menor que 0,05 ($p<0,05$). Para un nivel de confianza de 95%, que equivale a un valor $\alpha = 0,05$ se ha obtenido $T = 15,85$ con un valor $p < 0,05$ por lo que se rechaza la hipótesis nula

Paso 7. Interpretación y/o conclusión:

Como la hipótesis nula ha sido rechazada, se confirma que hay diferencias estadísticamente significativas en los procesos de auditoria y seguridad informática, dimensión gestión de riesgos, antes y después de la implementación de la metodología COBIT 5. Por lo que se concluye que la implementación de la metodología COBIT 5 mejora los procesos de auditoria y seguridad informática en la dimensión gestión de riesgos de la empresa.

Con respecto al objetivo específico 2

Paso 1. Objetivo específico 2

Identificar si hay diferencia en los procesos de auditoria y seguridad informática, dimensión seguridad informática, antes y después de la implementación de la metodología COBIT 5.

Paso 2. Hipótesis estadística

H_0: No hay diferencias estadísticamente significativas en los procesos de auditoria y seguridad informática, dimensión seguridad informática, antes y después de la implementación de la metodología COBIT 5.

H_1: Si hay hay diferencias estadísticamente significativas en los procesos de auditoria y seguridad informática, dimensión seguridad informática, antes y después de la implementación de la metodología COBIT 5.

Paso 3. Se determina el nivel de significación: Usando un nivel de significancia del 5% (α=0,05)

Paso 4. Se elige el estadígrafo de prueba: $$t = \frac{\overline{d}}{\sigma_d / \sqrt{n}}$$

Se trabajó con la prueba estadística T-Student, para muestras relacionadas, con un nivel de significación del 5% (p < 0,05).

Paso 5: Prueba para muestras relacionadas

TABLA N° 4: Resultados de las encuestas antes y después de la implementación de la metodología COBIT 5, dimensión seguridad informática**.**

Puntaje obtenido	**Antes**		**Después**	
	nº	**%**	**nº**	**%**
20 – 25	1		-	
25 – 30	7		-	
30 – 35	11		5	
35 – 40	1		13	
40 – 45	-		2	
Total	20	100	20	100
Media	30,25		36,30	
D.e.	2,95		2,41	

Fuente: Encuesta ejecutada por el investigador

PRE Y POST PRUEBA	DIFERENCIAS RELACIONADAS		PRUEBA T PARA IGUALDAD DE MEDIAS		
	Media	Desv. estándar	t	gl	Valor p
GRUPO EXPERIMENTAL	6,05	2,42	11,20	19	**0,0001**

Paso 6. Se determina regla de decisión:

Rechazar la Hipótesis nula si el valor p es menor que 0,05 ($p<0,05$). Para un nivel de confianza de 95%, que equivale a un valor $\alpha = 0,05$ se ha obtenido $T = 11,20$ con un valor $p < 0,05$ por lo que se rechaza la hipótesis nula

Paso 7. Interpretación y/o conclusión:

Como la hipótesis nula ha sido rechazada, se confirma que hay diferencias estadísticamente significativas en los procesos de auditoria y seguridad informática, dimensión seguridad informática, antes y después de la implementación de la metodología COBIT 5. Por lo que se concluye que la implementación de la metodología COBIT 5 mejora los procesos de auditoria y seguridad informática en la dimensión seguridad informática de la empresa.

Con respecto al objetivo específico 3

Se definió y se construyó las metas de cascada de COBIT 5 adaptados a la Empresa DATCO S&H la cual está en la parte de implementación, así como en anexo.

V. DISCUSIÓN

Luego de analizar los resultados obtenidos en el estudio realizado en la empresa DATCO S&H, a fin de determinar los niveles de madurez según el modelo COBIT en la gestión de las tecnologías de la información y las comunicaciones, se llegó a las siguientes conclusiones:

- Los resultados obtenidos en el presente estudio determinan que en la Empresa DATCO S&H, el nivel de proceso de definición del plan estratégico de las tecnologías de información y comunicaciones, es ubicado en el nivel crítico de la escala de madurez del modelo COBIT.
- Los resultados obtenidos en el presente estudio determinan que en la Empresa DATCO S&H, el nivel de administración de calidad de las IT, es ubicado en el nivel crítico de la escala de madurez del modelo COBIT.

VI. CONCLUSIONES

- ✓ El modelo de implementación de COBIT 5 propuesto contribuye alinear TI a los objetivos estratégicos de la empresa, incrementado funcionalidades de TI debido a que en el modelo propuesto estructura y esquematiza el conjunto de actividades (habilitadores) de cada proceso, esto hace mejorar los procesos de auditoria y seguridad informatica.
- ✓ Como se demostró, la hipótesis nula ha sido rechazada, se confirma que hay diferencias estadísticamente significativas en los procesos de auditoria y seguridad informática, dimensión gestión de riesgos, antes y después de la implementación de la metodología COBIT 5. Por lo que se concluye que la implementación de la metodología COBIT 5 mejora los procesos de auditoria y seguridad informática en la dimensión gestión de riesgos de la empresa.
- ✓ Como se demostró, la hipótesis nula ha sido rechazada, se confirma que hay diferencias estadísticamente significativas en los procesos de auditoria y seguridad informática, dimensión seguridad informática, antes y después de la implementación de la metodología COBIT 5. Por lo que se concluye que la implementación de la metodología COBIT 5 mejora los procesos de auditoria y seguridad informática en la dimensión seguridad informática de la empresa.
- ✓ Se definió y se construyó las metas de cascada de COBIT 5 adaptados a la Empresa DATCO S&H la cual está en la parte de implementación, así como en anexo.

VII. RECOMENDACIONES

- Utilizando COBIT 5, las empresas pueden fácilmente identificar datos sensitivos, asegurar que los datos estén seguros, demostrar cumplimiento con leyes y regulaciones aplicables, monitorear proactivamente los datos, y reaccionar y responder rápidamente a las brechas de datos y privacidad.
- Tomar las medidas respectivas necesarias para acortar la brecha entre el porcentaje de procesos realizados de manera aceptable contrastados con lo definido por la metodología COBIT 5.
- Continuar con la aplicación de la metodología COBIT 5, para el diagnóstico y evaluación de los procesos restantes pertenecientes a los dominios de Evaluar, Dirigir, Supervisar; Alinear, Planear, organizar; y Entrega, Servicio, Soporte; para garantizar la:
    - Optimización de los recursos de TI.
    - Disponibilidad de información oportuna, segura y confiable.
    - Infraestructura tecnológica robusta, escalable y rentable.
    - Actualizaciones puntuales, efectivas y eficaces.
    - Soporte a usuarios garantizados.
    - Protección de datos.
    - Recurso humano calificado.
    - Equilibrio entre los riesgos y las inversiones de TI.
    - Políticas y procedimientos adecuados para cada proceso.
- El eslabón más débil es la persona, por lo tanto, se debe concientizar y sensibilizar.

- Para que la metodología de las buenas prácticas se implemente, las partes interesadas deben involucrarse.

Lo anteriormente descrito permitirá a DATCO S&H, alcanzar todo el potencial que promete la tecnología, generando un clima de confianza con los directivos y sus clientes, y contribuir en el logro de los objetivos estratégicos de la organización.

VIII. REFERENCIAS BIBLIOGRAFICAS

ACHA ITURMENDI, J. (1994). *Auditoria Informática en las Empresas.* Parainfo.

COSTAS SANTOS, J. (2010). *Seguridad informática.* Madrid: Ra-Ma.

DEL PESO, E. (Julio de 2001). *La Auditoría de los Sistemas de Información.* Obtenido de http://www.iee.es

ECHENIQUE, J. (s.f.). Obtenido de http://campus.uab.es/~2082564/indice2.htm

HEREDERO, C., López Hermoso Agius, J. J., Romo Romero, S. M., & Medina Salgado, S. (2013). *Organización y transformación de los sistemas de información en la empresa.* ALFAOMEGA.

ISACA. (2012). Obtenido de http://www.isaca.org

ISACA. (2012). *COBIT 5 Implementación.*

ISACA. (2012). *COBIT 5 Procesos Catalizadores.*

ISACA. (2012). *COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de la Empresa.*

ISACA. (s.f.). *COBIT 5: Otras Guías de catalizadores*. Obtenido de www.isaca.org/cobit

MUÑOZ SERNA, R., & MARTINEZ ARIAS, M. (2012). *Caracterización de Procesos de Gestión de TI basados en COBIT 5, para la implemenmtación en la industria Editorial Colombiana.* Santiago de Cali.

PRADO OSEGUERA, D. M. (2009). *Metodología para el establecimiento de objetivos de control como un medio de seguridad en el Área de Tecnologías de Información.* Mexico.

SOLIZ, A., & GEOVANNI, J. (2012). *Auditoria de Riesgos informáticos del departamento de sistemas de Caves SAEMA utilizando COBIT como marco de referencia.* Sangolqui.

ANEXO

MATRIZ DE CONSISTENCIA LÓGICA

"APLICACIÓN DE LA METODOLOGÍA COBIT 5 PARA LA MEJORA DE PROCESOS DE AUDITORIA Y SEGURIDAD INFORMÁTICA EN LA EMPRESA DATCO S&H"

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES	METODOLOGÍAS
¿En qué medida se mejorará la Auditoría y Seguridad Informática en la empresa DATCO S&H con la aplicación de la metodología COBIT 5?	GENERAL: Implementar la metodología COBIT 5 para mejorar los procesos de auditoria y seguridad informática en la empresa DATCO S&H. ESPECÍFICOS: Identificar si hay diferencia en los procesos de auditoria y seguridad informática, dimensión gestión de riesgos, antes y después de la implementación de la metodología COBIT 5. Identificar si hay diferencia en los procesos de auditoria y seguridad informática, dimensión seguridad informática, antes y después de la implementación de la metodología COBIT 5.	Con la implementación de la metodología COBIT 5 se mejora los procesos de auditoria y seguridad informática en la empresa DATCO S&H.	V.I: Metodología COBIT 5 V.D: Procesos de Auditoria y seguridad informática	TIPO: Explicativa DISEÑO: Cuasi experimental longitudinal MÉTODOS DE INVESTIGACIÓN: Experimental, cuantitativo ESTRATEGIAS O PROCEDIMIENTOS DE RECOGIDA DE INFORMACIÓN: Recopilación de la bibliografía relacionada con los estándares de calidad internacionales: COBIT, ISO/IEC 12207, ISO/IEC 27002 (antes 17799), ISO/IEC 20000 Y PMBOK. Elaboración de la metodología para la auditoría integral de la gestión informática. Aplicación de la metodología para la auditoría integral de la gestión informática.

	Definir y construir las Metas de Cascada de COBIT 5			Afinamiento de la metodología. Aplicación de la metodología afinada. Evaluación de los resultados. Se evaluó el impacto resultante de la aplicación de la metodología para la auditoría integral de la gestión informática. ANÁLISIS E INTERPRETACIÓN DE LA INFORMACIÓN: Para contrastar la hipótesis se hizo uso de la estadística inferencial, para ello se tuvo en cuenta el análisis de la estadística paramétrica con la prueba T-Student para muestras relacionadas, con un nivel de significación del 5% ($p<0,05$). INSTRUMENTOS: Encuestas realizadas a los colaboradores de la Empresa DATCO S&H, gestores de los activos informáticos. UNIDAD DE ANÁLISIS: La unidad de análisis es un gestor responsable del control de los activos de información antes mencionados con las vulnerabilidades y amenazas que

				enfrentan, el impacto que tendría en la organización una eventual falla de éste, así como la gestión que se está realizando con cada uno de ellos. ANÁLISIS DE DATOS: Los datos que se obtengan con los instrumentos serán evaluados en base a la técnica de análisis cuantitativo. DISEÑO DE LA VALIDACIÓN DE LA HIPOTESIS: Se hará mediante la comparación en cuanto a tiempo y calidad de resultados, para lo cual se deben comparar los resultados obtenidos por diferentes métodos: Aplicación de encuestas para la medición de desempeño de los procesos involucrados con las variables de la investigación en dos momentos: Pre y Post prueba. El juicio de Expertos. Controles que se desarrollara como parte del presente trabajo.

MATRIZ DE CONSISTENCIA DE VALORACIÓN - VARIABLE DEPENDIENTE

INDICADOR	PESO %	Nº DE ITEMS	VALORACIÓN MÁXIMA DEL ITEM	VALORACIÓN MÁXIMA DEL INDICADOR
1	19%	7	5	35
2	8%	3	5	15
3	14%	5	5	25
4	24%	9	5	45
5	5%	2	5	10
6	11%	4	5	20
7	19%	7	5	35
8	0%	0	0	0
9	0%	0	0	0
10	0%	0	0	0
TOTAL	**100%**	**37**	**5**	**185**

Fuente: Elaboración propia

NIVELES DE GESTIÓN DE RIESGOS Y SEGURIDAD INFORMÁTICA

VALOR	CALIFICACIÓN	VALOR INFERIOR	VALOR SUPERIOR
5	Muy Bueno	148	185
4	Bueno	111	148
3	Medio	74	111
2	Malo	37	74
1	Muy Malo	0	37

Fuente: Elaboración propia

RANGO DE VALORACIÓN: POR INDICADOR Y DIMENSIÓN - VARIABLE DEPENDIENTE

NIVELES	I1		I2		I3		I4		D1		I5		I6		I7		D2		ENCUESTADO	
	[LI	LS>	[LI	LS>	[LI	LS>	[LI	LS>	[LI	LS>	[LI	LS>	[LI	LS>	[LI	LS>	[LI	LS>	[LI	LS>
Muy Bueno	28	35	12	15	20	25	36	45	96	120	8	10	16	20	28	35	52	65	**148**	**185**
Bueno	21	28	9	12	15	20	27	36	72	96	6	8	12	16	21	28	39	52	**111**	**148**
Medio	14	21	6	9	10	15	18	27	48	72	4	6	8	12	14	21	26	39	**74**	**111**
Malo	7	14	3	6	5	10	9	18	24	48	2	4	4	8	7	14	13	26	**37**	**74**
Muy Malo	0	7	0	3	0	5	0	9	0	24	0	2	0	4	0	7	0	13	**0**	**37**

RANGO DE VALORACIÓN DE NIVELES POR TOTAL DE ENCUESTADOS: POR INDICADOR, DIMENSIÓN Y MUESTRA - VARIABLE DEPENDIENTE

NIVELES	I1		I2		I3		I4		D1		I5		I6		I7		D2		MUESTRA	
	[LI	LS>	[LI	LS>	[LI	LS>	[LI	LS>	[LI	LS>	[LI	LS>	[LI	LS>	[LI	LS>	[LI	LS>	[LI	LS>
Muy Bueno	**560**	**700**	240	300	400	500	**720**	**900**	1920	2400	160	200	**320**	**400**	560	700	1040	1300	**2960**	**3700**
Bueno	**420**	**560**	180	240	300	400	**540**	**720**	1440	1920	120	160	**240**	**320**	420	560	780	1040	**2220**	**2960**
Medio	**280**	**420**	120	180	200	300	**360**	**540**	960	1440	80	120	**160**	**240**	280	420	520	780	**1480**	**2220**
Malo	**140**	**280**	60	120	100	200	**180**	**360**	480	960	40	80	**80**	**160**	140	280	260	520	**740**	**1480**
Muy Malo	**0**	**140**	0	60	0	100	**0**	**180**	0	480	0	40	**0**	**80**	0	140	0	260	**0**	**740**

Fuente: Elaboración propia

Tamaño de Muestra	**20**

MATRIZ DE OPERACIONALIZACIÓN DE VARIABLES

Variable		Dimensiones	Indicadores	Items	Valoración
V.D. Procesos de Auditoría y Seguridad Informática	Proceso administrativo que consiste en mejorar y optimizar actividades donde intervienen las TI.	**Gestión de Riesgos:** Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.	Políticas de Seguridad	**1,2,3,4,5,6,7**	Muy Malo, Malo, Medio, Bueno y Muy Bueno
			Gestión de Activos	**8,9,10**	Muy Malo, Malo, Medio, Bueno y Muy Bueno
			Amenazas	**11,12,13,14,15**	Muy Malo, Malo, Medio, Bueno y Muy Bueno
			Vulnerabilidades	**16,17,18,19,20,21,22,23,24**	Muy Malo, Malo, Medio, Bueno y Muy Bueno
		Seguridad Informática: Protección de la confidencialidad, integridad y disponibilidad de los activos de información según sea necesario para alcanzar los objetivos de negocio de la organización.	Integridad	**25,26**	Muy Malo, Malo, Medio, Bueno y Muy Bueno
			Confidencialidad	**27,28,29,30**	Muy Malo, Malo, Medio, Bueno y Muy Bueno
			Disponibilidad	**31,32,33,34,35,36,37**	Muy Malo, Malo, Medio, Bueno y Muy Bueno

V.I Metodología COBIT 5	Metodología de buenas prácticas para gobierno de TI	**Adaptar COBIT 5**: Actividades para crear un artefacto COBIT 5 Quickstart.	Marco de Referencia COBIT 5	1,2,3,4,5,6,7	Muy Malo, Malo, Medio, Bueno y Muy Bueno
			COBIT 5 Quickstart	8,9,10	Muy Malo, Malo, Medio, Bueno y Muy Bueno
		Implementar COBIT 5: Actividades para implementar COBIT 5	Políticas de Seguridad	11,12,13,14,15,16,17	Muy Malo, Malo, Medio, Bueno y Muy Bueno
			Gestión de Activos	18,19,20	Muy Malo, Malo, Medio, Bueno y Muy Bueno
			Amenazas	21,22,23,24,25	Muy Malo, Malo, Medio, Bueno y Muy Bueno
			Vulnerabilidades	26,27,28,29,30,31,32,33,34	Muy Malo, Malo, Medio, Bueno y Muy Bueno

Valoración:

1. Muy Malo 2. Malo 3. Medio 4. Bueno 5. Muy Bueno

Fuente: Elaboración propia.

ANEXO 01: ENCUESTA - METODOLOGÍA COBIT 5 (VARIABLE INDEPENDIENTE)

1. Marco de referencia COBIT 5.	S	F	A	M	N
1. ¿DATCO S&H cuenta con políticas y procedimientos de seguridad de COBIT?					
2. ¿Cuenta DATCO S&H con una normativa referida a la seguridad de la información Alineada a COBIT?					
3. ¿Conoce las políticas o normas de seguridad de la información de COBIT 5?					
4. ¿Las políticas, normas y procedimientos de seguridad de la información cuenta con personal responsable de dichos instrumentos que entienda COBIT 5?					
5. ¿Sabe que brinda el Estándar COBIT 5?					
6. ¿Conoce que son buenas practicas?					
7. ¿Conoce algún marco de trabajo o estándar sobre gestión de TI?					
2. COBIT 5 Quickstart	**S**	**F**	**A**	**M**	**N**
8. ¿Conoce el COBIT Quickstart?					
9. ¿En que beneficia COBIT Quickstart ?					
10. ¿Sera necesario crear COBIT Quickstart?					
3. Políticas de seguridad de la información.	**S**	**F**	**A**	**M**	**N**
11. ¿DATCO S&H cuenta con políticas y procedimientos de seguridad formalmente documentadas y aprobadas por la Gerencia?					
12. ¿Cuenta DATCO S&H con una normativa referida a la seguridad de la información?					
13. ¿Las políticas o normas de seguridad de la información se revisan y actualizan periódicamente de acuerdo a las nuevas necesidades presentes?					
14. ¿Las políticas, normas y procedimientos de seguridad de la información cuenta con personal responsable de dichos instrumentos?					
15. ¿Los requerimientos de la red para el control de accesos se tienen formalmente definidas y documentadas?					
16. ¿Las reglas y los derechos del control de accesos, para cada usuario o grupo de usuarios, se deben establecio claramente en una declaración de política de accesos?					
17. ¿Se desarrollan e implementan planes de contingencia ante desastres que permitan el funcionamiento y operatividad de la red?					
4. Gestión de activos	**S**	**F**	**A**	**M**	**N**
18. ¿Se realizan inventarios de todos los equipos y software asociados a la red de DATCO S&H?					
19. ¿Todos los activos asociados a la Red DATCO S&H cuentan con un propietario asignado?					
20. ¿Los activos de DATCO S&H se encuentran inventariados y cuenta con un propietario nombrado?					
5. Amenazas	**S**	**F**	**A**	**M**	**N**
21. ¿Las áreas de servidores y cuartos de comunicaciones se encuentran protegidas adecuadamente contra amenazas físicas externas (inundaciones, incendios, explosiones, corte de líneas y suministros, terremotos, huelgas...)?					
22. ¿Se tienen procedimientos para notificación y gestión de incidencias?					
23. ¿Han ocurrido incidentes en la red de DATCO S&H					
24. ¿Las instalaciones cuentan con sistema de alarma por presencia de fuego, humo, así como extintores de incendio, conexiones eléctricas seguras, entre otras?					
25. ¿Se detectan rápidamente los incidentes de seguridad ocurridos en la Red de DATCO S&H?					
6. Vulnerabilidades	**S**	**F**	**A**	**M**	**N**
26. ¿La red de DATCO S&H se encuentra segregada en dominios lógicos?					
27. ¿Se ejecutan planes para la formación de los usuarios de la red en materia de seguridad de la información?					
28. ¿Reciben los usuarios de la red la información la adecuada formación y actualización regular en las políticas, normas y procedimientos de seguridad de la información?					
29. ¿Se realizan campañas para la concientización de los usuarios acerca del uso adecuado de los servicios de la red?					
30. ¿Existen mecanismos para la comunicación a los usuarios de las normas y procedimientos de seguridad de la información?					
31. ¿Se posee una clara descripción de los atributos de seguridad de todos los servicios de red utilizados por la organización?					
32. ¿Se realizan evaluaciones de riesgos de seguridad de la información en la Red DATCO S&H?					
33. ¿Se gestionan los riesgos de seguridad informática en la Red DATCO S&H?					
34. ¿Se tienen herramientas para el monitoreo de los sistemas y los equipos conectados a la Red DATCO S&H?					

ANEXO 02: ENCUESTA PROCESOS DE AUDITORÍA Y SEGURIDAD INFORMÁTICA (VARIABLE DEPENDIENTE)

1. Políticas de seguridad de la información.	S	F	A	M	N
1. ¿DATCO S&H cuenta con políticas y procedimientos de seguridad formalmente documentados y aprobados por la Gerencia?					
2. ¿Cuenta DATCO S&H con una normativa referida a la seguridad de la información?					
3. ¿Las políticas o normas de seguridad de la información se revisan y actualizan periódicamente de acuerdo a las nuevas necesidades presentes?					
4. ¿Las políticas, normas y procedimientos de seguridad de la información cuenta con personal responsable de dichos instrumentos?					
5. ¿Los requerimientos de la red para el control de accesos se tienen formalmente definidas y documentadas?					
6. ¿Las reglas y los derechos del control de acceso, para cada usuario o grupo de usuarios, se tienen establecido claramente en una declaración de política de accesos?					
7. ¿Se desarrollan e implementan planes de contingencia ante desastres que permitan el funcionamiento y operatividad de la red?					
2. Gestión de activos	**S**	**F**	**A**	**M**	**N**
8. ¿Se realizan inventarios de todos los equipos y software asociados a la red de DATCO SAU?					
9. ¿Todos los activos asociados a la Red DATCO S&H cuentan con un propietario asignado?					
10. ¿Los activos de DATCO SAU se encuentran inventariados y cuenta con un propietario nombrado?					
3. Amenazas	**S**	**F**	**A**	**M**	**N**
11. ¿Las áreas de servidores y cuartos de comunicaciones se encuentran protegidas adecuadamente contra amenazas físicas externas (inundaciones, incendios, explosiones, cortes de línea y sabotajes, terremotos, huelgas ...)?					
12. ¿Se tienen procedimientos para notificación y gestión de incidencias?					
13. ¿Han ocurrido incidentes en la red de DATCO SAU					
14. ¿Las instalaciones cuentan con sistema de alarma por presencia de fuego, humo, así como extintores de incendio, conexiones eléctricas seguras, entre otros?					
15. ¿Se detectan rápidamente los incidentes de seguridad ocurridos en la Red de DATCO SAU?					
4. Vulnerabilidades	**S**	**F**	**A**	**M**	**N**
16. ¿La red de DATCO S&H se encuentra segregada en dominios lógicos?					
17. ¿Se ejecutan planes para la formación de los usuarios de la red en materia de seguridad de la información?					
18. ¿Reciben los usuarios de la red la información la adecuada formación y actualización regular en las políticas, normas y procedimientos de seguridad de la información?					
19. ¿Se realizan campañas para la concientización de los usuarios acerca del uso adecuado de los servicios de la red?					
20. ¿Existen mecanismos para la comunicación a los usuarios de las normas y procedimientos de seguridad de la información?					
21. ¿Se posee una clara descripción de los atributos de seguridad de todos los servicios de red ofrecidos por la organización?					
22. ¿Se realizan evaluaciones de riesgos de seguridad de la información en la Red DATCO S&H?					
23. ¿Se gestionan los riesgos de seguridad informática en la Red DATCO S&H?					
24. ¿Se tienen herramientas para el monitoreo de los sistemas y los equipos conectados a la Red DATCO S&H?					
5. Integridad	**S**	**F**	**A**	**M**	**N**
25. ¿Los servidores y equipos de comunicaciones se mantienen en habitaciones cerradas con acceso limitado a personas autorizadas?					
26. ¿Existen mecanismos para la detección, prevención y protección de la red contra códigos maliciosos?					
6. Confidencialidad	**S**	**F**	**A**	**M**	**N**
27. ¿Existen acuerdos de confidencialidad o no divulgación de la información, con personal de DATCO SAU y terceros?					
28. ¿Se le informa a los usuarios de la red que deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas?					
29. ¿Los usuarios de la red tienen acceso a los servicios para los cuales han sido específicamente autorizados?					
30. ¿Existen controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red?					
7. Disponibilidad	**S**	**F**	**A**	**M**	**N**
31. ¿En caso de variación de voltaje o cortes de energía se tienen instalado equipos que protejan la información y los dispositivos como: reguladores de voltaje, supresores de pico, sistemas de almacenaje con motor amperio (UPS), generadores de energía?					
32. ¿Se ejecutan planes de mantenimiento preventivo y correctivo de la infraestructura de hardware y software asociados a la Red DATCO SAU?					
33. ¿Se realizan proyecciones de los requerimientos de la capacidad futura de los sistemas a ser implementados dentro de la Red DATCO S&H, asegurando la disponibilidad y desempeño requerido del sistema?					
34. ¿Se realizan copias de seguridad de toda la información esencial de DATCO S&H?					
35. ¿Se realiza, mantiene y garantiza la integridad de la información a través de procedimientos de respaldos?					
36. ¿Se Planifica el mantenimiento y la actualización de los equipos y sistemas que permitan el acceso a los servicios de información en producción?					
37. ¿Se cuenta en la Red DATCO S&H con controles especiales para mantener la disponibilidad de los servicios de red y equipos conectados?					

OBJETIVOS DE LA EMPRESA

Objetivos de la Empresa de COBIT 5

Dimensión del CMI	Objetivo de la Empresa	
Financiera	1	Valor para las Partes Interesadas de las Inversiones de Negocio
	2	Cartera de productos y servicios competitivos
	3	Riesgos de negocio gestionados (salvaguarda de activos)
	4	Cumplimiento de leyes y regulaciones externas
	5	Transparencia financiera
Cliente	6	Cultura de servicio orientada al cliente
	7	Continuidad y disponibilidad del servicio de negocio
	8	Respuestas ágiles a un entorno de negocio cambiante
	9	Toma estratégica de Decisiones basada en Información
	10	Optimización de costes de entrega del servicio
Interna	11	Optimización de la funcionalidad de los procesos de negocios
	12	Optimización de los costes de los procesos de negocio
	13	Programas gestionados de cambio en el negocio
	14	Productividad operacional y de los empleados
	15	Cumplimiento con las políticas internas
Aprendizaje y Crecimiento	16	Personas preparadas y motivadas
	17	Cultura de innovación de producto y negocio

OBJETIVOS DE LAS TI

METAS RELACIONADAS CON LAS TI

Dimensión del CMI TI	Meta de Información y Tecnología Relacionada	
Financiera	1	Alineamiento de TI y estrategia de negocio
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI
	4	Riesgos de negocio relacionados con las TI gestionados
	5	Realización de beneficios del portafolio de inversiones y Servicios relacionados con las TI
	6	Trasparencia de los costes, beneficios y riesgos de las TI
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas
Interna	9	Ágilidad en las TI
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
	11	Optimización de activos, recursos y capacidades de las TI
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad
	14	Disponibilidad de información útil y fiable para la toma de decisiones
	15	Cumplimiento de las políticas internas por parte de las TI
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado
	17	Conocimiento, experiencia e iniciativa para la innovación de negocio

METAS CORPORATIVAS DE COBIT 5

Dimensión del CMI	Metas Corporativas	Relación con los Objetivos de Gobierno		
		Realización de Beneficios	Optimización de Riesgos	Optimización de Recursos
Financiera	1. Valor para las partes interesadas de las inversiones de Negocio	P		S
	2. Cartera de productos y servicios competitivos	P	P	S
	3. Riesgos de negocio gestionados (salvaguarda de activos)		P	S
	4. Cumplimiento de leyes y regulaciones externas		P	
	5. Transparencia financiera	P	S	S
Cliente	6. Cultura de servicio orientada al cliente	P		S
	7. Continuidad y disponibilidad del servicio de negocio		P	
	8. Respuestas ágiles a un entorno de negocio cambiante	P		S
	9. Toma estratégica de Decisiones basada en información	P	P	P
	10. Optimización de costes de entrega del servicio	P		P
Interna	11. Optimización de la funcionalidad de los procesos de negocio	P		P
	12. Optimización de los costes de los procesos de negocio	P		P
	13. Programas gestionados de cambio en el negocio	P	P	S
	14. Productividad operacional y de los empleados	P		P
	15. Cumplimiento con las políticas internas		P	
Aprendizaje y Crecimiento	16. Personas preparadas y motivadas	S	P	P
	17. Cultura de innovación de producto y negocio	P		

METAS RELACIONADAS CON TI CORRESPONDEN A METAS CORPORATIVAS

Analizando qué metas relacionadas con TI corresponden a estas metas corporativas

			META CORPORATIVA																
			Valor para los interesados de las inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de decisiones basada en información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personas preparadas y motivadas	Cultura de innovación de producto y negocio
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	Meta relacionada con las TI		Financiera					Cliente					Interna					Aprendizaje y crecimiento	
Financiera	1	Alineamiento de TI y la estrategia de negocio	P	P	S			P	S	P	P	S	P	S	P			S	S
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P											P		
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	4	Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	5	Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI	P	P				S		S		S	S	P		S			S
	6	Transparencia de los costes, beneficios y riesgos de las TI	S		S		P				S	P		P					
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interna	9	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10	Seguridad de la información, infraestructuras de procesamiento y aplicaciones			P	P			P								P		
	11	Optimización de activos, recursos y capacidades de las TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	P	S	S			S				S		S	P				
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de TI con las políticas internas			S	S											P		
Aprendizaje y desarrollo	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P				S		P	S		S		S			S	P

PARTES INTERESADAS Y METAS CORPORATIVAS

Esta tabla se puede usar para establecer y priorizar metas corporativas específicas o relacionadas con TI, basadas en las necesidades de las partes interesadas

NECESIDADES DE LAS PARTES INTERESADAS	Valor para los interesados de las inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de decisiones basada en información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personas preparadas y motivadas	Cultura de innovación de producto y negocio
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
¿Cómo se consigue valor mediante el uso de TI? ¿Está el usuario final satisfecho con la calidad del servicio de TI?	■	■				■	■						■			■	■
¿Cómo se gestiona el rendimiento de TI?		■			■				■	■	■	■		■			
¿Cómo se puede explotar mejor la tecnología de red para conseguir nuevas oportunidades estratégicas?	■	■						■					■			■	■
¿Cómo puedo construir y estructurar mejor mi departamento de TI?								■		■	■	■		■	■	■	
¿Cuánto dependo de mis proveedores externos? ¿Cómo de bien están siendo gestionados los acuerdos de externalización de TI? ¿Cómo puedo verificarlos sobre proveedores externos?			■	■						■							
¿Cuáles son los requisitos (de control) para la información				■					■						■		
¿He contemplado todo los riesgos relacionados con TI?			■				■		■						■		
¿Estoy ejecutando una operación de TI eficiente y robusta?					■		■										
¿Cómo se controla el coste de TI? ¿Cómo se usan los recursos de TI en la manera más efectiva y eficiente? ¿Cuáles son las opciones de aprovisionamiento más efectivas y eficientes?										■		■		■			
¿Tengo suficiente personal para TI? ¿Cómo puedo desarrollar y mantener sus habilidades y cómo gestiono su										■		■		■			
¿Cómo consigo confianza sobre TI?				■											■		
¿Está bien securizada la información que se está procesando?				■			■								■		
¿Cómo se puede mejorar la capacidad de respuesta del negocio mediante un entorno de TI más flexible?	■							■								■	■
¿Fracasan los proyectos de TI en proporcionar lo que habían prometido? Si es así, ¿Por qué permanece la TI en el camino de ejecutar la estrategia de negocio?	■	■	■					■			■	■	■				
¿Cómo es de crítica la TI para la sostenibilidad de la empresa? ¿Qué pasaría si la TI no estuviera disponible?	■	■					■										
¿Qué procesos de negocio críticos dependen de TI y cuáles son los requerimientos de los procesos de negocio?	■	■									■	■					
¿En cuánto ha excedido de media los presupuestos de operación de TI? ¿Con qué frecuencia y cuánto se salen del presupuesto los proyectos de TI?					■					■		■		■			
¿Qué parte del esfuerzo de TI se dedica a apagar fuegos en lugar de facilitar las mejoras del negocio?		■	■									■					
¿Son suficientes los recursos y la infraestructura de TI disponibles para conseguir los objetivos estratégicos de empresa requeridos?		■			■					■		■					
¿Cuánto se tarda en la toma de decisiones importantes de TI?	■				■			■									
¿Son transparentes el esfuerzo y las inversiones totales en TI?		■		■	■										■		
¿Respalda TI a la empresa en el cumplimiento de la normativa y los niveles de servicio? ¿Cómo puedo saber si se cumple con todas las normas aplicables?				■											■		