FACULTAD DE CIENCIAS CONTABLES, ECONÓMICAS Y FINANCIERAS
SECCIÓN DE POSGRADO

LA AUDITORIA INTERNA Y SU INCIDENCIA EN LA OPTIMIZACIÓN DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LOS USUARIOS DEL SISTEMA SAP DE LAS EMPRESAS DE SERVICIOS LOGÍSTICOS EN LA PROVINCIA CONSTITUCIONAL DEL CALLAO, AÑO 2016-2017

PRESENTADA POR

RAÚL ENRIQUE VALDIVIA CASTAÑEDA

ASESOR

DEMETRIO PEDRO DURAND SAAVEDRA

TESIS

PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN CIENCIAS CONTABLES Y FINANCIERAS CON MENCIÓN EN GESTIÓN DE RIESGOS Y AUDITORÍA INTEGRAL

LIMA – PERÚ

2019

FACULTAD DE CIENCIAS CONTABLES, ECONÓMICAS Y FINANCIERAS

SECCIÓN DE POSGRADO

LA AUDITORIA INTERNA Y SU INCIDENCIA EN LA OPTIMIZACIÓN DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACION DE LOS USUARIOS DEL SISTEMA SAP DE LAS EMPRESAS DE SERVICIOS LOGÍSTICOS EN LA PROVINCIA CONSTITUCIONAL DEL CALLAO, AÑO 2016-2017.

TESIS

PARA OBTENER EL GRADO ACADÉMICO DE MAESTRO EN CIENCIAS CONTABLES Y FINANCIERAS CON MENCIÓN EN GESTION DE RIESGOS Y AUDITORIA INTEGRAL

PRESENTADO POR

RAUL ENRIQUE VALDIVIA CASTAÑEDA

LIMA, PERÚ

2019

“LA AUDITORIA INTERNA Y SU INCIDENCIA EN LA OPTIMIZACIÓN DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACION DE LOS USUARIOS DEL SISTEMA SAP DE LAS EMPRESAS DE SERVICIOS LOGÍSTICOS EN LA PROVINCIA CONSTITUCIONAL DEL CALLAO, AÑO 2016-2017”

ASESOR Y MIEMBROS DEL JURADO

ASESOR:

Dr. Demetrio Pedro Durand Saavedra

PRESIDENTE DEL JURADO:

Dr. Juan amadeo Alva Gómez

SECRETARIO:

Dr. Cristian Alberto Yong Castañeda

MIEMBROS DEL JURADO:

Dra. Olga Victoria Aguilar Barco Celis

Dr. Alonso Rojas Mendoza

Dr. Luz Rosanna Lapa Salinas

DEDICATORIA

A Dios sobre todas las cosas por darme la fuerza para continuar en este proceso de obtener uno de mis anhelos más deseados.

A mis padres y abuelos ejemplos de trabajo y sacrificio y con mucho cariño a mi esposa Carla y mi hija Camila.

AGRADECIMIENTO

A mis profesores quienes me guiaron y condujeron hacia la culminación exitosa de mi Tesis, a quienes agradezco por sus consejos y guías para el perfeccionamiento de la misma.

En especial, a mi asesor de esta tesis, Doctor Pedro Durand Saavedra por su comprensión y enseñanza.

ÍNDICE

CAPÍTULO II : MARCO TEÓRICO

CAPÍTULO III : HIPOTESIS Y VARIABLES

CAPÍTULO IV : METODOLOGIA

RESUMEN

Este trabajo de investigación está referida a la necesidad de implementar la auditoría interna con la finalidad de optimizar o mejorar la Gestión de Seguridad de la Información de los usuarios del sistema SAP de las Empresas de Servicios Logísticos, se basó principalmente en la existencia de empresas que adolecen de mecanismos de control para el otorgamiento de los accesos y privilegios en el sistema SAP, esta es ocasionada por una inadecuada gestión de seguridad generando el riesgo de que usuarios no autorizados procesen trabajos de forma indebida, lo cual podría afectar la integridad, disponibilidad y confidencialidad de la información.

En la investigación, se planteó como objetivo, determinar si la Auditoria Interna incide en la optimización de la Gestión de Seguridad de la Información de los Usuarios del sistema SAP en Empresas de Servicios Logísticos en la provincia constitucional del Callao, para lo cual se buscó información de interés para desarrollar la presente tesis.

En cuanto a la estructura del trabajo, abarco desde el planteamiento del problema, marco teórico, metodología, resultados, discusión, conclusiones y recomendaciones; respaldada por una amplia fuente de información, quienes con sus aportes ayudaron a clarificar la problemática en referencia, destacando que las variables son de importancia actual.

Al terminar la investigación, se pudo concluir que la Auditoría Interna incide favorablemente en la optimización de la Gestión de Seguridad de la Información de los usuarios del sistema SAP en Empresas de Servicios Logísticos en la provincia constitucional del Callao a través de sus técnicas y procedimientos de auditoria, a fin de detectar conflictos de segregación de funciones, prevenir errores o fraudes en la asignación de los usuarios e identificando riesgos a los que se encuentra expuesta la información sensible y estas sean asumidas, gestionadas y minimizadas por las organizaciones.

Palabras claves: Auditoría, Seguridad de la Información, Gestión.

ABSTRACT

This research work refers to the need to implement internal auditing in order to optimize or improve the Management of Information Security of users of the SAP system of Logistics Services Companies, was based mainly on the existence of companies that suffer from control mechanisms for granting access and privileges in the SAP system, this is caused by inadequate security management generating the risk that unauthorized users process work improperly, which could affect the integrity, availability and confidentiality of information.

In the investigation, it was proposed as objective, to determine if the Internal Audit influences in the optimization of the Management of Security of the Information of the Users of the SAP system in Companies of Logistic Services in the constitutional province of the Callao, for which information of interest was looked for to develop the present thesis.

As for the structure of the work, I cover from the statement of the problem, theoretical framework, methodology, results, discussion, conclusions and recommendations; supported by a wide source of information, who with their contributions helped to clarify the problem in reference, emphasizing that the variables are of current importance.

At the end of the investigation, it was possible to conclude that the Internal Audit positively affects the optimization of the Management of Information Security of the Users of the SAP system in Logistics Services Companies in the constitutional province of Callao through its audit techniques and procedures, in order to detect conflicts of segregation of functions, errors in the assignment of users and identifying risks to which the sensitive information is exposed and these are assumed, managed and minimized by the organizations.

Keywords: Audit, Information Security, Management.

INTRODUCCION

La tesis tiene como título de desarrollo: “La Auditoría Interna y su incidencia en la optimización de la Gestión de Seguridad de la Información de los usuarios del sistema SAP de las empresas de servicios logísticos en la provincia constitucional del Callao, año 2016-2017”, la cual fue estructurada en seis capítulos: Planteamiento del Problema, Marco Teórico, Hipótesis y Variables, Metodología, Resultados, terminando con la Discusión, Conclusiones y recomendaciones, acompañada de una amplia fuente bibliográfica, la misma que sustenta el desarrollo de esta investigación; así como los anexos correspondientes.

Capitulo I: Planteamiento del Problema, en este punto abarca la metodología empleada para el desarrollo de la tesis; incluyendo la descripción de la realidad problemática, delimitaciones, problemas, objetivos, justificación e importancia del trabajo, limitaciones; terminando con la viabilidad del estudio.

Capitulo II: Marco teórico, abarca desde los antecedentes, marco legal, marco teórico con sus respectivas conceptualizaciones sobre; la auditoria interna y la gestión de la seguridad de la información; donde cada una de las variables se desarrolló con el apoyo de material procedente de especialistas.

Capitulo III: Hipótesis y Variables, se expone la formulación de las hipótesis y su respectiva Operacionalización de las variables de la investigación.

Capitulo IV: Metodología, comprende desde el tipo, nivel, método, diseño; así como la población y muestra, técnicas de recolección de datos, técnicas de procesamiento de datos y aspectos éticos.

Capitulo V: Análisis e Interpretación de Resultados, se trabajó con la técnica del cuestionario con preguntas cerradas, con las cuales se realizó la parte estadística y gráfica; además se interpretó preguntas por pregunta, facilitando una mayor comprensión, culminando con la contrastación de las hipótesis.

Capitulo V: Discusión, Conclusiones y Recomendaciones, en cuanto a la discusión, se analiza la parte teórico conceptual y normatividad existente relacionada con las variables, las conclusiones que se realizaron de acuerdo a la formulación de los objetivos y en cuanto a las recomendaciones se puede apreciar que son viables y practicables de acuerdo a la metodología y algunas consideraciones de las entrevistas.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

Actualmente las organizaciones empresariales, principalmente las empresas de servicios logísticos, en su mayoría su proceso organizacional se desarrolla tanto a nivel de Oficina Principal y Sucursales; siendo su principal preocupación es la gestión de los usuarios en los sistemas integrados denominados ERP que para nuestra investigación comprende el sistema SAP (Systems, Applications, Products in data Procesing), el cual es reconocido mundialmente como uno de los mejores ERP siendo utilizado por grandes corporaciones sin embargo, es la administración de cada organización que debe implementar controles adecuados con el fin de establecer que ninguna persona debe tener demasiados accesos y privilegios a un sistema que le permita ejecutar transacciones en todo un proceso de negocios sin controles ni autorizaciones.

Permitir este tipo de acceso representa un riesgo muy real para los negocios y manejar este riesgo de manera pragmática y eficaz es más difícil.

Dentro de este contexto, las compañías tratan de identificar en la medida de lo posible cumplir con la segregación de funciones la cual preocupa principalmente a los departamentos de Tecnologías de la Información (TI), Auditoría Interna y Finanzas. En gran medida, la dificultad radica en la complejidad y variedad de los sistemas que automatizan los procesos de negocios clave tales como: Caja, Facturación, Planillas, Compras, etc. así como; en la titularidad y responsabilidad del control de dichos procesos.

La segregación de funciones es un principio básico al control interno que busca asegurar que ninguna persona tenga la autoridad para ejecutar dos o más transacciones sensibles en conflicto que podrían afectar los estados financieros. Sin una guía adecuada y un enfoque razonable, podría parecer extremadamente difícil lograr implementar, probar, remediar y mitigar la segregación de funciones.

Entre otras situaciones que adolecen las empresas sobre el control de los usuarios es la falta de políticas, procedimientos y estándares formalmente establecidos, la cual permitan identificar los procesos claves de los negocios y clasificar por niveles de criticidad, la inadecuada asignación de los importes de liberación o autorización de los usuarios en los procesos, tales en las Áreas de Finanzas y Compras; asimismo, la falta de un maestro de usuarios que no sea validada por el Área de Recursos Humanos lo que podría a incurrir en pagos de licencias del personal cesado, existiendo el riesgo del uso indebido de estas cuentas de usuarios en operaciones no

autorizadas, afectando económicamente a las empresas; así como, en la fuga de información confidencial en poder de terceros.

La importancia de la Auditoría Interna en las organizaciones empresariales, radica principalmente en que las normas, procedimientos y estrategias que se utilizan, permite optimizar la gestión y desde luego tomar las decisiones más coherentes a nivel organizar, lo cual redunda en los resultados previstos.

Finalmente podemos decir, que las empresas no necesitan crear estructuras complejas de funciones ni realizar cambios costosos a fin de cumplir con la segregación de funciones y el principio del mínimo privilegio. Al enfocarse en las transacciones que presentan el mayor riesgo para el negocio, las compañías pueden entender rápidamente los problemas relacionados con el acceso e identificar a un nivel que satisfaga a la administración y a aquellos involucrados en la auditoría, si se están tomando las medidas adecuadas para corregir y mitigar las causas raíz de los problemas de segregación de funciones y accesos, motivo por el cual el suscrito, se propone investigar como la Auditoría Interna incide en la optimización de la gestión de seguridad de la información de los usuarios del sistema SAP.

De acuerdo, al análisis que hemos realizado los problemas que se producen en nuestra investigación se refieren a los Planes de Seguridad, que sirven para la prevención y/o acciones correctivas ante posibles contingencias en la asignación de Usuarios SAP, el Logro de Objetivos y Metas, que apunta hacia una adecuada madurez en el uso de la información registrada en el sistema SAP, Evaluar el Grado de Aceptación del Riesgo, que corresponden a aquellos riesgos que aceptan los negocios a fin de poder operar,

Efectividad de las Operaciones, que permita medir el desempeño de la gestión de seguridad de la asignación de usuarios SAP, el Grado de Eficiencia y Eficacia, que es el otorgamiento de nuevos usuarios SAP al personal que se realiza, en base a un análisis de costo-beneficio y por último, el Fortalecimiento de Políticas y Normas de la Seguridad de la Información, que es el propósito fundamental para una gestión adecuada Gestión de Seguridad de la información de los usuarios del sistema SAP.

DELIMITACION DE LA INVESTIGACION

Luego de haber descrito la problemática seleccionada con el tema a continuación con fines metodológicos; el estudio lo delimite en los siguientes aspectos:

1.1.1. Delimitación espacial

El estudio se llevó a cabo a nivel de empresas de servicios logísticos en la Provincia Constitucional del Callao.

1.1.2. Delimitación temporal

El periodo en cual se llevó a cabo la investigación abarcó del año 2016-2017.

1.1.3. Delimitación social

La técnica destinada al de recojo de datos se aplicó al personal de auditores y funcionarios que trabajan en la empresas de servicios logísticos.

1.1.4. Delimitación conceptual

a. Auditoría Interna

Es una actividad independiente y objetiva de aseguramiento y consulta concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y

disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

b. Gestión de Seguridad de la Información

Es la protección de la información contra una amplia gama de amenazas para asegurar la continuidad del servicio, incluye la estructura organizacional, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y recursos.

En nuestra investigación, tiene por objeto de implementar un modelo de autorizaciones de perfiles de usuarios SAP, a fin de reducir los riesgos de seguridad en el uso del sistema SAP y lograr una efectiva y eficiente administración en el acceso del sistema SAP.

1.2 FORMULACIÓN DEL PROBLEMA

1.2.1 Problema Principal

¿De qué manera la Auditoría Interna incide en la optimización de la Gestión de Seguridad de la Información de los usuarios del sistema SAP de las empresas de servicios logísticos en la Provincia Constitucional del Callao, año 2016-2017?

1.2.2 Problemas Secundarios

a. ¿De qué manera el grado de independencia y objetividad incide en el plan de seguridad de la información de los usuarios del sistema SAP?

b. ¿En qué medida el nivel de aporte de valor agregado incide en el logro de los objetivos y metas de la Gestión de Seguridad de la información de los usuarios del sistema SAP?

c. ¿En qué medida el nivel del sistema de control interno incide en el grado de aceptación del riesgo de la organización en la Gestión de Seguridad de la información de los usuarios del sistema SAP?

d. ¿En qué medida las acciones de control incide en la efectividad de las operaciones de la Gestión de Seguridad de la información de los usuarios del sistema SAP?

e. ¿De qué manera el seguimiento de las recomendaciones incide en el grado de eficiencia y eficacia de la Gestión de Seguridad de la información de los usuarios del sistema SAP?

f. ¿En qué medida los informes de auditoría incide en el fortalecimiento de las políticas y normas de la seguridad de la información de los usuarios del sistema SAP?

1.3 OBJETIVOS DE LA INVESTIGACIÓN

1.3.1 Objetivo General

Determinar si la Auditoría Interna incide en la optimización de la Gestión de Seguridad de la Información de los usuarios del sistema SAP de las empresas de servicios logísticos en la Provincia Constitucional del Callao, año 2016-2017.

1.3.2 Objetivos Específicos

a. Evaluar si el grado de independencia y objetividad incide en el plan de seguridad de la información de los usuarios del sistema SAP.

b. Establecer si el nivel de aporte de valor agregado incide en el logro de los objetivos y metas de la Gestión de Seguridad de la información de los usuarios del sistema SAP.

c. Analizar si el nivel del sistema de control interno incide en el grado de aceptación del riesgo de la organización en la Gestión de Seguridad de la información de los usuarios del sistema SAP.

d. Definir si las acciones de control incide en la efectividad de las operaciones de la Gestión de Seguridad de la información de los usuarios del sistema SAP.

e. Comprobar si el seguimiento de las recomendaciones incide en el grado de eficiencia y eficacia de la Gestión de Seguridad de la información de los usuarios del sistema SAP.

f. Demostrar si los informes de auditoría incide en el fortalecimiento de las políticas y normas de la seguridad de la información de los usuarios del sistema SAP.

1.4 JUSTIFICACIÓN DE LA INVESTIGACIÓN

La presente investigación se justifica por cuanto brinda la formulación de las medidas de control para la Gestión de la Seguridad de los Usuarios del sistema SAP en las empresas de servicios logísticos, propone un modelo de autorizaciones SAP, la cual permita la administración y control de los accesos de manera óptima.

Por su aplicación en las empresas de servicios logísticos esta investigación se establece un conjunto de actividades con el propósito de identificar los principales problemas y formular un modelo de autorizaciones que permita la administración y control de los accesos de manera óptima.

Algunos aspectos importantes como lo son la formalización de responsabilidades por puesto o función, los procedimientos de autorización y los responsables de la realización de los controles, devenidos de una adecuada segregación de funciones; se consideran como aspectos críticos y, por ende, se enfoca en la presente investigación.

1.4.1 Importancia

La presente investigación desarrollada es importante por cuanto está encaminado a identificar y evaluar riesgos de seguridad a nivel de autorizaciones en el sistema SAP con impacto en los procesos de los negocios, reduciendo a un nivel aceptable para el negocio, los riesgos de seguridad a nivel de autorizaciones de los usuarios SAP y además permitirá plantear normas y procedimientos apropiados a esta actividad.

El aporte de esta investigación proporcionará medidas para reducir los riesgos e seguridad a nivel de autorizaciones en el uso del sistema SAP lo que se lograra una efectiva y eficiente administración de las autorizaciones en el sistema

SAP, controlando que los accesos al sistema SAP sean asignados y actualizados de acuerdo a las actividades que realizan los empleados.

Asimismo, optimizará los tiempos de atención a los requerimientos e incidentes de los usuarios relacionados las autorizaciones y mejorar el cumplimiento con los requerimientos de información para las actividades de auditoría de procesos de negocio, auditoría de licenciamiento SAP e investigaciones sobre incidentes de seguridad.

1.4.2 Viabilidad de la Investigación

El trabajo de investigación es viable debido a que se contó con la información necesaria para su desarrollo; así como también los medios económicos, logísticos y bibliográficos para llevar a cabo.

1.5 LIMITACIONES

No existe limitaciones para el desarrollo del presente trabajo de investigación, ya que se cuenta con las facilidades para lograr culminarlo de la mejor manera posible, existen fuentes escritas y orales con las cuales se sustentara la veracidad de este trabajo de investigación.

CAPÍTULO II

MARCO TEÓRICO

2.1 ANTECEDENTES DE LA INVESTIGACIÓN

En la consulta llevada a cabo a nivel de las Facultades de Ciencias Contables, Económicas y Financieras y Escuelas de Post Grado, se ha determinado que en relación al tema no existen otros estudios que hayan tratado sobre dicha problemática, por lo cual considero que el trabajo en referencia reúne las condiciones metodológicas y temáticas suficientes para ser considerada novedosa.

Sin embargo, dentro de las averiguaciones realizadas, se encontraron las siguientes investigaciones, que sin referirse directamente al tema, constituyen referencias de interés a tomar en consideración, entre las cuales tenemos:

2.1.1. Universidades peruanas

a. Universidad de San Martín de Porres

Autor: PRADO PALOMINO, Jorge

Título: ***La Auditoría Interna en la optimización del Gobierno Corporativo a nivel de una Empresa de Producción de Biocombustibles"*** (2013), para obtener el

grado académico de Maestro en Auditoría y Control de Gestión Empresarial

Resumen:

El desarrollo de la tesis, trató sobre la importancia de la actividad de Auditoría Interna en las organizaciones que se desarrolle aplicando el nuevo marco de la Auditoría Interna, con independencia y objetividad, que brinde aseguramiento y consultoría, y agregue valor y mejora en las operaciones, teniendo como responsabilidad evaluar y hacer recomendaciones apropiadas para la mejora de los procesos de gobierno corporativo.

Como parte de su función de aseguramiento, teniendo como objetivos principales: promover la ética y valores, asegurar la gestión y responsabilidad en el desempeño, comunicar información de riesgos y control, y coordinar las actividades y la información de comunicación entre la administración, Auditoría y la dirección.

b. Universidad Nacional Federico Villarreal

Autor: PADILLA CANO, Marco

Título: ***"Auditoría interna para una adecuada ejecución presupuestaria en la Clínica Hogar de la Madre"*** (2009), para obtener el grado académico de Maestro en Auditoría Contable y Financiera

Resumen:

Esta investigación establece que la Auditoría Interna aporta un examen objetivo del área presupuestaria mediante la aplicación de procedimientos que permitan obtener evidencia suficiente, competente y relevante para luego informar y recomendar procedimientos para el control previo, concurrente y posterior; y,

otros aspectos para viabilizar la ejecución presupuestara de la Clínica Hogar de la Madre.

La necesidad de la Auditoría Interna se pone de manifiesto en una empresa a medida que ésta aumenta en volumen, extensión geográfica y complejidad y hace imposible el control directo de las operaciones por parte de la dirección. Con anterioridad, el control lo ejercía directamente la dirección de la empresa por medio de un permanente contacto con sus mandos intermedios, y hasta con los empleados de la empresa. En la gran empresa moderna esta peculiar forma de ejercer el control ya no es posible hoy día, y de ahí la emergencia de la llamada Auditoría Interna.

c. Universidad de San Martín de Porres

Autor: ARGOTE LAZÓN, Lina

Título: ***"Auditoría Interna y la mejora de gestión en las empresas constructoras de Lima Metropolitana, año 2011"*** (2013), para obtener el grado académico de Maestro en Auditoría y Control de Gestión Empresarial

Resumen:

Tiene por objetivo, de implementar el grado de importancia que las empresas constructoras tengan implementado una Área de Auditoría Interna con el propósito de coadyuvar a que la gestión de las empresa medianas del sector construcción cumpla con los objetivos y el rol de las operaciones de tal forma que constituya una valiosa herramienta que ayudaría en la toma decisiones y fortalecimiento de los controles internos.

Asimismo, menciona que el rol de la Auditoría Interna en la empresa constructoras, así como en otras realizan actividades lucrativas permite identificar los riesgos a que están expuestos las organizaciones empresariales para que la gerencia implemente un

sistema de control interno con la finalidad de evitar contingencias económicas futuras que podrían afectar su sostenibilidad en el tiempo.

d. Universidad de San Martín de Porres

Autor: GAGO RIOS, Rosario

Título: ***"La implementación de Auditoría Interna y su impacto en la gestión de las cooperativas de servicios múltiples de Lima Metropolitana"*** (2013), para obtener el grado académico de Maestro en Auditoría y Control de Gestión Empresarial

Resumen:

Esta tesis tuvo como principal objetivo, determinar si la implementación de un área de Auditoría Interna influye en los resultados de la gestión financiera de las cooperativas de servicios múltiples de Lima Metropolitana, concluyendo que a través de sus técnicas, procedimientos de Auditoría, contribuyen en la detección de los errores a fin de aplicar las medidas correctivas o preventivas para mejorar la situación actual de estas organizaciones.

Es necesario que las cooperativas de servicios múltiples de Lima Metropolitana implementen un área de Auditoría Interna en sus organizaciones, dadas las dificultades que presentan éstas en sus procesos y procedimientos, los mismos no corregidos pueden traer como consecuencia la no continuidad y sostenibilidad de estas instituciones.

e. **Universidad Nacional Daniel Alcides Carrión**

Autor: MURGUIA SANTOS, Evelyn

Título: ***"Impacto de la auditoría de los estados financieros de inventarios en la gestión financiera de la Unidad de***

Gestión Educativa Local (UGEL).” (2012), para obtener el grado académico de Maestro en Auditoría Integral.

Resumen:

Esta investigación indica que la Auditoría, no se preocupa de registrar, resumir, presentar ni de comunicar dichas transacciones; su objetivo fundamental es revisar la forma en la cual las transacciones y situaciones económico-financieras que afectan a la empresa han sido tanto medidas como comunicadas.

Asimismo, es tarea de la Auditoría determinar la adecuación y fiabilidad de los sistemas de información y de las políticas y procedimientos operativos existentes en los distintos departamentos de la empresa; en definitiva la Auditoría cubre todas las funciones de revisión, utilizando a la contabilidad como el vehículo más idóneo para realizarla.

f. **Universidad de San Martin de Porres**

Autor: SUAREZ ARISPE, Oscar Juan

Título: ***“Administración en el asignamiento de roles y transacciones en el sistema ERP SAP/R3 del grupo Química Suiza S.A.”*** (2005), para obtener el grado académico de Título de Ingeniero en Computación y Sistemas.

Resumen:

Esta tesis tuvo como principal objetivo, la implantación para la empresa Química Suiza S.A de una herramienta de última generación como SAP/R3 que le va a respaldar en los procesos críticos de la empresa de acuerdo a una adecuada asignación de roles y transacciones de acuerdo a las funciones y responsabilidades de los usuarios.

De esta forma los conflictos generados por los usuarios, son controlados mediante el desarrollo de técnicas de análisis y seguimiento para los diferentes perfiles de usuarios, permitiendo generar documentación y reduciendo costos de operación para la empresa.

2.1.2. Universidades extranjeras

a. Universidad Javeriana (Colombia)

Autor: BERMUDEZ ROJAS, Patricia

Título: ***"El contador público y la Auditoría Interna"*** (2010), para obtener el grado académico de Maestro en Auditoría.

Resumen:

Tiene como objetivo, determinar que la Auditoría Interna, es una actividad dentro de la Empresa para la evaluación de la organización y el control y para la revisión de las operaciones, en especial de aquellas que tienen repercusión en la información contable y financiera como base para proporcionar un servicio a la dirección; es un órgano dependiente de la administración, que funciona con el propósito de evaluar y vigilar la efectividad de los controles establecidos por la administración; en últimas, es un control de controles.

También refiere el autor que la función primordial de la Auditoría Interna es la de vigilar los controles establecidos en la empresa mediante la revisión de la información contable y financiera y de la evaluación de la organización, para detectar los problemas del control interno y establecer las medidas de protección de los intereses de la compañía, promoviendo simultáneamente la eficiencia de la operación.

b. **Universidad Autónoma de Querétaro (México)**

Autor: QUIÑONES SÁNCHEZ, Juan

Título: ***"Control y manejo de seguridad para el sistema ERP (SAP), por medio de la definición de roles transaccionales"*** (2013), para obtener el grado académico de Maestro en Sistemas de Información: Gestión y Tecnología.

Resumen:

Esta tesis tuvo como principal objetivo, implementar un sistema de información que permita auditar de manera periódica las operaciones que se ejecutan en el sistema SAP, por medio de los empleados de la compañía, y tener la posibilidad de establecer medidas preventivas y mejoramiento que contribuyan a reducir el número de conflictos a nivel planta.

El éxito de la compañía depende principalmente de la calidad de la información y de la velocidad con que pueda ser compartida, es por esto que administrar la seguridad informática es de vital importancia para el crecimiento empresarial. Estableciendo procedimientos para identificar los tipos de conflictos que generan los empelados al ejecutar transacciones en el sistema SAP.

c. **Universidad Carlos III de Madrid (España)**

Autor: GARCÍA CÁMARA, Javier

Título: ***"Seguridad y Auditorías Aplicadas al Módulo de Gestión de Tiempos de SAP HR"*** (2011), para obtener el grado académico de Título de Ingeniero de Telecomunicación.

Resumen:

Esta tesis tuvo como principal objetivo, implementar el estándar para la seguridad de la información ISO 27002 en el punto 11.3, vigente desde julio de 2007, debe buscarse como objetivo evitar el

acceso al sistema de usuarios no autorizados, evitando poner en peligro la información y sus medios de procesamiento. En esta tarea se considera fundamental la colaboración del usuario y hace hincapié en el uso de contraseñas secretas.
Este trabajo pretende servir de documento de referencia para aquellas personas que se van a enfrentar a una auditoría, pero también puede ser de utilidad a aquellos profesionales que tengan que realizar una implantación SAP o se vean inmersos en un proyecto relacionado con la gestión de autorizaciones.

d. **Universidad Instituto Politécnico Nacional (México)**

Autor: IZQUIERDO GARCIA, Alejandra

Título: ***"Auditoría al Módulo CRM de SAP de Corporación Industrial HRC"*** (2010), para obtener el grado académico de Título de Ingeniero en Computación e Informática.

Resumen:
Tiene por objetivo, explicar los controles generales de seguridad de información del módulo CRM dentro del ERP SAP para emitir recomendaciones a Corporación HRC con base a las buenas prácticas de la industria.

Con el trabajo realizado, se cuenta con un panorama general de las vulnerabilidades y de los posibles impactos en caso de que se materialice una amenaza, siendo la información uno de los activos más importantes para la empresas que en su mayoría, hoy en día, hace uso de la Tecnología de Información; por lo tanto es necesario contar con procesos definidos y procedimientos de administración de usuarios y privilegios, que ayuden a salvaguardar la integridad, confidencialidad y disponibilidad de la información que conlleven a brindar soporte y dar valor al negocio.

2.1.3. MARCO LEGAL

AUDITORÍA INTERNA

a. **Ley Nº 13253 promulgada el 11 de setiembre de 1959 - "Ley de Profesionalización del Contador Público",** con relación a la Auditoría señala lo siguiente:

Art. 1º.- Modifíquese el Art. 35º del Código de Comercio en los siguientes términos:

"Art. 35º.- Los Comerciantes deberán llevar sus libros de Contabilidad con la intervención de Contadores titulados Públicos o Mercantiles".

Art. 4º.- Corresponde a los Contadores Públicos efectuar y autorizar toda clase de balances, peritajes y tasaciones de su especialidad, operaciones de Auditoría y estudios contables con fines judiciales y administrativos. Corresponde a los Contadores Mercantiles, además de las atribuciones que le concede el Art. 1º de esta Ley, autorizar balances con fines tributarios.

Art. 5º.- Es obligatoria la colegiación de los Contadores Públicos en los lugares donde ejerzan actividades profesionales 10 o más titulados. Los Colegios vigilarán la observancia de las normas de ética profesional, propenderán al mejoramiento de la profesión y a la ayuda mutua entre sus asociados. Cada Colegio formulará sus propios estatutos que deberán ser aprobados por el Ministerio de Hacienda y Comercio.

Art. 8º.- En caso de que las facultades señaladas por esta Ley, sean ejercidas por una asociación o sociedad de contadores, sus informes y actuaciones deberán ser refrendados por uno o más contadores Públicos que la representen, quienes serán responsables solidariamente con la respectiva entidad.

b. **Ley N° 28951 promulgada el 16 de enero del 2007 - "Ley de Actualización de la Ley 13253 de Profesionalización del Contador Público y de creación de los Colegios de Contadores Públicos"**, con relación a la Auditoría señala lo siguiente:

Art. 3º.- Competencias de Contador Público son las siguientes:

a. Planificar, organizar, supervisar y dirigir la contabilidad general y de costos de las actividades económico- comerciales desarrolladas por personas naturales y/o jurídicas del ámbito privado, público o mixto y formular, autorizar y/o certificar los estados financieros

correspondientes, incluidos los que se incorporen a la declaraciones juradas y otros para fines tributarios.

b. Evaluar, asesorar y realizar consultoría en sistemas de contabilidad computarizada y de control y otros relacionados con el ejercicio de la profesión contable.

c. Realizar auditoría financiera, tributaria, exámenes especiales y otros inherentes a la profesión de contador público.

d. Efectuar el peritaje contable en los procesos judiciales, administrativos y extrajudiciales.
e. Certificar el registro literal de la documentación contable incluyendo las partidas o asientos contables de los libros o registros contables de las personas naturales y jurídicas.

f. Formular valuaciones y tasaciones de naturaleza contable.

c. **Ley N° 28755 – Ley que modifica el artículo 366° de la Ley N° 25702, incorpora una disposición final y complementaria, y modifica los artículos 198°, 244° y 245° del Código penal**, promulgada el 6 de junio 2006, con relación a la Auditoría señala lo siguiente:

Artículo N° 3.- La modificación de los artículos 198°, 244 y 245 del Código Penal cuyos textos está relacionado con el auditor y gerente es el siguiente:

"Artículo N° 198° Administración fraudulenta.
Será reprimido con pena privativa de libertad no menor de un ni mayor de cuatro años el que, en su condición de fundador, miembro del directorio o del consejo de administración o del consejo de vigilancia, gerente, administrador, auditor interno,

auditor externo o liquidador de una persona jurídica, realiza, en perjuicio de ella o de terceros.

Artículo 245.- Ocultamiento, omisión o falsedad de información.
El director, gerente, administrador, representante legal, miembro del consejo de administrador, miembro del consejo de vigilancia, miembro del comité de crédito, auditor interno, auditor externo, liquidador o funcionario de institución bancaria, financiera u otra que opere con fondos del público, que con el propósito de ocultar situaciones de liquidez o insolvencia de la institución, omita o niegue proporcionar información o proporcione datos falsos a las autoridades de control y regulación, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años y con ciento ochenta a trescientos sesenta y cinco días- multa[12]

d. **Las NAGAS** tienen su origen en los Boletines (Statement on Auditing Estándar – SAS) emitidos por el Comité de Auditoría del Instituto Americano de Contadores Públicos de los Estados Unidos de Norteamérica publicadas en el año 1948.

   En el Perú, se aprobaron en octubre de 1968 con motivo del II Congreso de Contadores, que tuvo lugar en la ciudad de Lima. Posteriormente, se ha ratificado su aplicación en el III Congreso Nacional de Contadores, que se celebró en 1971 en la ciudad de Arequipa. Detallamos:

   <u>Normas Generales o Personales</u>

   1. Entrenamiento y capacidad profesional
   2. Independencia
   3. Cuidado o esmero profesional.

   <u>Normas de Ejecución del Trabajo</u>

   4. Planeamiento y Supervisión
   5. Estudio y Evaluación del Control Interno
   6. Evidencia Suficiente y Competente

Normas de Preparación del Informe

7. Aplicación de los Principios de Contabilidad Generalmente Aceptados.
8. Consistencia
9. Revelación Suficiente
10. Opinión del Auditor

e. **Normas Internacional de Auditoría (NIAs)** Estas normas han sido emitidas por la International Federation OF Accountants (IFAC) entidad que fue creada en 1977 para uniformar la normativa de los diferentes países. La NIAs constituye un requisito formal que debe cumplir el auditor.

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

a. Con fecha 23 de julio del 2004 la Presidencia del Consejo de Ministros (PCM) a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), **dispone el uso obligatorio de la Norma Técnica Peruana *"NTP – ISO/IEC 17799:2004 EDI. Tecnología de la Información: Código de Buenas Prácticas para la Gestión de la Seguridad de la Información"*** en entidades del Sistema Nacional de Informática. Se actualizó el 25 de Agosto del 2007 con la **Norma Técnica Peruana "NTP – ISO/IEC 17799:2007 EDI.**

Es una compilación de recomendaciones para las prácticas exitosas de seguridad, que toda organización puede aplicar independientemente de su tamaño o sector, fue redactada para que fuera flexible y no induce a las organizaciones que la cumplan al pie de la letra, se deja a estas dar una solución de seguridad de acuerdo a sus necesidades.

Las recomendaciones de la NTP-ISO 17799 son neutrales en cuanto a la tecnología. La norma discute la necesidad de contar con Firewalls, pero no profundiza sobre los tipos de Firewalls y

cómo se utilizan. En este sentido La Norma Técnica Peruana ISO – 17799, se emite para ser considerada en la implementación de estrategias y planes de seguridad de la información de las Entidades Públicas.

Cabe señalar, que la norma no exige la certificación, pero si la consideración y evaluación de los principales dominios de acuerdo a la realidad de cada organización. De la misma, se consideran 11 dominios de control:

1. Política de seguridad:

Se necesita una política que refleje las expectativas de la organización en materia de seguridad, a fin de suministrar administración con dirección y soporte. La política también se puede utilizar como base para el estudio y evaluación en curso.

2. Aspectos organizativos para la seguridad:

Sugiere diseñar una estructura de administración dentro la organización, que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes.

3. Clasificación y Control de Activos:

Inventario de los recursos de información de la organización y con base en este conocimiento, debe asegurar que se brinde un nivel adecuado de protección.

4. Seguridad de Recursos Humanos:

Necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de

seguridad y asuntos de confidencialidad. Implementa un plan para reportar los incidentes.

5. Seguridad física y del Entorno:

Responde a la necesidad de proteger las áreas, el equipo y los controles generales.

6. Gestión de Comunicaciones y Operaciones:

Los objetivos de esta sección son:

- Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.
- Minimizar el riesgo de falla de los sistemas.
- Proteger la integridad del software y la información.
- Conservar la integridad y disponibilidad del procesamiento y la comunicación de la información.
- Garantizar la protección de la información en las redes y de la infraestructura de soporte.
- Evitar daños a los recursos de información e interrupciones en las actividades de la institución.
- Evitar la pérdida, modificación o uso indebido de la información que intercambian las organizaciones.

7. Control de accesos:

Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación como protección contra los abusos internos e intrusos externos.

8. Adquisición, Desarrollo y Mantenimiento de los sistemas:

Recuerda que en toda labor de la tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad en todas las etapas del proceso.

9. Gestión de Incidentes de la Seguridad de la información

Asegurar que los eventos y debilidades en la seguridad de la información sean comunicados de manera que permitan una acción correctiva a tiempo.

10. Gestión de Continuidad del Negocio

Aconseja estar preparado para contrarrestar las interrupciones en las actividades de la organización y para proteger los procesos importantes de la organización en caso de una falla grave o desastre.

11. Cumplimiento:

Evitar brechas de cualquier ley civil o criminal, estatutos, obligaciones regulatorias o contractuales y de cualquier requerimiento de seguridad.

b. **EL COBIT** que son los Objetivos de Control para Información y Tecnologías Relacionadas (COBIT, en inglés: Control Objectives for Information and related Tecnología) es una guía de mejores prácticas presentado como framework, dirigida al control y supervisión de tecnología de la información (TI). Mantenido por ISACA (en inglés: Information Systems Audit and Control Association) y el IT GI (en inglés: IT Governance Institute), tiene una serie de recursos que pueden servir de modelo de referencia para la gestión de TI, incluyendo un resumen ejecutivo, un framework, objetivos de control, mapas de auditoría, herramientas para su implementación y principalmente, una guía de técnicas de gestión.

La misión de COBIT es "investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que sean autorizados (dados por alguien con autoridad), actualizados, e internacionales para el uso del día a día de los gestores de negocios (también directivos) y auditores". Gestores, auditores, y usuarios se benefician del desarrollo de COBIT porque les ayuda a entender sus Sistemas de Información (o tecnologías de la información) y decidir el nivel de seguridad y control que es necesario para proteger los activos de sus compañías mediante el desarrollo de un modelo de administración de las tecnologías de la información.

La primera edición fue publicada en 1996; la segunda edición en 1998; la tercera edición en 2000 (la edición on-line estuvo disponible en 2003); y la cuarta edición en diciembre de 2005, y la versión 4.1 está disponible desde mayo de 2007. Actualmente el COBIT se encuentran con la versión 5 se lanzó el 10 de abril de 2012 la nueva edición de este marco de referencia. COBIT 5 es la última edición del framework mundialmente aceptado, el cual proporciona una visión empresarial del Gobierno de TI que tiene a la tecnología y a la información como protagonistas en la creación de valor para las empresas.

c. **NTP-ISO/IEC 27001:2005** es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission. Es una norma de carácter internacional que tiene como objetivo garantizar que los controles que existen para salvaguardar la información de las partes interesadas son adecuados para proteger la

confidencialidad, integridad y disponibilidad de la información. Estos controles deben tener en cuenta la información de clientes, empleados, socios, y las necesidades de la sociedad en general.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como “Ciclo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

Beneficios que aporta este a los objetivos de la organización:

- Demuestra la garantía independiente de los controles internos y cumple los requisitos de gestión corporativa y de continuidad de la actividad comercial.

- Demuestra independientemente que se respetan las leyes y normativas que sean de aplicación.

- Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial.

- Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información.

- Demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información.

La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance, entendiendo por alcance el ámbito de la organización que va a estar sometido al Sistema de Gestión de la Seguridad de la Información elegido. En general, es recomendable la ayuda de consultores externos.

2.2 BASES TEORICAS

RESEÑA HISTORICA – AUDITORIA INTERNA

La Auditoría es reconocida desde los tiempos más remotos, teniéndose conocimientos de su existencia ya en las lejanas épocas de la civilización sumeria. La Auditoría proviene del verbo latino audire, que significa oír. Los romanos utilizaron este término para controlar en nombre del emperador, sobre la gestión de las Provincias.

El hecho de que los soberanos exigieran el mantenimiento de las cuentas de su residencia por dos escribanos independientes, pone de manifiesto que fueron tomadas algunas medidas para evitar desfalcos en dichas cuentas.

A medida que se desarrolló el comercio, surgió la necesidad de las revisiones independientes para asegurarse de la adecuación y finalidad de los registros mantenidos en varias empresas comerciales. La auditoría como profesión fue reconocida por primera vez bajo la Ley Británica de Sociedades Anónimas de 1862 y el reconocimiento general tuvo lugar durante el período de mandato de la Ley “Un sistema metódico y normalizado de

contabilidad era deseable para una adecuada información y para la prevención del fraude".

También reconocía "Una aceptación general de la necesidad de efectuar una versión independiente de las cuentas de las pequeñas y grandes empresas". Desde 1862 hasta 1905, la profesión de la auditoría creció y floreció en Inglaterra, y se introdujo en los Estados Unidos hacia 1900. En Inglaterra se siguió haciendo hincapié en cuanto a la detección del fraude como objetivo primordial de la auditoría.

En 1912 Montgomery dijo: "En los que podría llamarse los días en los que se formó la auditoría, a los estudiantes se les enseñaban que los objetivos primordiales de ésta eran: La detección y prevención de fraude".

Este cambio en el objetivo de la auditoría continuó desarrollándose, no sin oposición, hasta aproximadamente 1940. En este tiempo "Existía un cierto grado de acuerdo en que el auditor podía y debería no ocuparse primordialmente de la detección de fraude". El objetivo primordial de una auditoría independiente debe ser la revisión de la posición financiera y de los resultados de operación como se indica en los estados financieros de los clientes, de manera que pueda ofrecerse una opinión sobre la adecuación de estas presentaciones a las partes interesadas.

Paralelamente al crecimiento de la auditoría independiente en los Estados Unidos, se desarrollaba la Auditoría Interna y del Gobierno, lo que entró a formar parte del campo de la auditoría. A medida que los auditores independientes se apercibieron de la importancia de un buen sistema de control interno y su relación con el alcance de las pruebas a efectuar en una auditoría independiente, se mostraron partidarios del crecimiento de los

departamentos de auditoría dentro de las organizaciones de los clientes, que se encargaría del desarrollo y mantenimiento de unos buenos procedimientos del control interno, independientemente del departamento de contabilidad general.

La auditoría gubernamental fue oficialmente reconocida en 1921 cuando el Congreso de los Estados Unidos estableció la Oficina General de contabilidad.

La crisis de Wall Street de Estados Unidos en 1929 y la creación de la Securities and Exchange Commission (SEC), órgano regulador y controlador de la Bolsa, han sido factores determinantes para conseguir las cotas de desarrollo que los profesionales de la auditoría han alcanzado en aquel país.

En el caso de España la introducción de la profesión de la auditoría ha sido muy lenta, en 1943 nace el Instituto de Censores Jurados de Cuentas de España (ICJCE) y, más recientemente, el Registro de Economistas Auditores (REA) en 1982 y el Registro General de Auditores (REGA) en 1985.

Así progresivamente, las compañías adoptaron la expansión de las actividades del departamento de Auditoría Interna hacia áreas que están más allá del alcance de los sistemas contables.

En nuestros días, los departamentos de Auditoría Interna se dedican a las revisiones de todas las fases de las corporaciones, de las que las operaciones financieras forman parte. (Cashin, Neuwirth y Levy, 1985).

2.2.1 VARIABLE INDEPENDIENTE

X: AUDITORIA INTERNA

Para Arens Alvin y James Loebbecke (2010), en su libro Auditoría Un Enfoque Integral; señalan que la auditoría operacional es una revisión de cualquier parte del proceso y métodos de operación de una compañía con el propósito de evaluar su eficiencia y eficacia. Al término de una auditoría operacional, es común que la administración espere algunas recomendaciones para mejorar sus operaciones. (p.5)

Comentario:

Entonces según, Arens Alvin y James Loebbecke señalan que la Auditoría Interna es un proceso de validación que brinda seguridad razonable de las operaciones basándose de los lineamientos establecidos por la Dirección y las Gerencias, con el propósito de evaluar la eficiencia y eficacia de los controles para alcanzar el adecuado cumplimiento de los objetivos estratégicos de la empresa, asimismo, como valor agregado de la labor de Auditoría aporta recomendaciones que contribuyan en el mejoramiento de las operaciones.

Para el Instituto de Auditores Internos de España (2013), en su libro Marco Internacional para la práctica Profesional de la Auditoría Interna, señala que la Auditoría Interna, es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización.

La Auditoría Interna, ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar los procesos de gestión de riesgos, control y gobierno. (p.17)

Comentario:

Según el Instituto de Auditores Internos de España, considera que la función de Auditoría Interna en una entidad, es una actividad independiente de evaluación, que permite examinar y evaluar la suficiencia y efectividad de la estructura del control interno de las empresas, bajo un enfoque basado en la gestión de riesgos y gobierno corporativo. Cabe señalar, que los Auditores Internos reportan a los más altos directivos de la empresa; por lo que, la independencia es importante para el cumplimiento de los objetivos trazados.

Por su parte, Juan Santillana (2013) en su libro Auditoría Interna Integral, señala que la Auditoría Interna es una función que coadyuva con la organización en el logro de sus objetivos; para ello se apoya en una metodología sistemática para analizar los procesos de negocio y las actividades y procedimientos relacionados con los grandes retos de la organización, que deriva en la recomendación de soluciones.

La Auditoría Interna es una función practicada por auditores internos profesionales con un profundo conocimiento en la cultura de negocios, los sistemas y los procesos. La función de Auditoría Interna provee seguridad de que los controles internos instaurados son adecuados para mitigar los riesgos y alcanzar el logro de las metas y objetivos de la organización.

Con base en la aplicación de un enfoque que asegure eficiencia en los procesos de administración de riesgos, de control y gobierno, es propósito de la Auditoría Interna entregar a la alta administración resultados cualitativos, cuantitativos, independientes, confiables, oportunos y objetivos además de asistir a las organizaciones públicas y privadas a alcanzar sus metas y objetivos.

El alcance de la función de la Auditoría Interna en una organización es amplio e involucra aspectos como los siguientes: revisar y evaluar la eficiencia en las operaciones, la confiabilidad de la información financiera y operativa, determinar e investigar fraudes, las medidas de protección de activos y el cumplimiento con leyes y regulaciones involucra también el asegurar apego a las políticas y los procedimientos instaurados en la organización. Es importante señalar que los auditores internos no son responsables de la ejecución de las actividades de la organización por lo que sólo proponen a la administración y el consejo de administración (o su equivalente) medidas para el mejor desempeño de las responsabilidades de éstos.

Como resultado del gran alcance de la función de Auditoría Interna, los auditores internos deben contar con amplios conocimientos y sólida formación académica y profesional. (p.11)

Comentario:

Es así, que Juan Santillana afirma que la Auditoría Interna es una función independiente de evaluación establecida dentro de una organización tiene por objetivo fundamental examinar y evaluar la adecuada y eficaz aplicación de los sistemas de control interno, velando por la preservación e integridad de los activos; así como, la eficiencia de su gestión económica, proponiendo recomendaciones a la dirección a fin de comunicar las acciones correctivas. Para ello, su alcance de su función es dar confiabilidad a las operaciones financiera, la salvaguarda de los activos y los cumplimientos de las políticas y procedimientos. Es importante señalar, que para la ejecución óptima del proceso de la Auditoría Interna es necesario contar con un conocimiento profundo del negocio, la que contribuye a establecer los alcances y objetivos de labor de la Auditoría; así como, con la experiencia adquirida el Auditor Interno adquiere nuevos conocimientos que agregan valor a la empresa.

Del mismo modo, la Universidad de Buenos Aires (2008) en su Manual de Auditoría Interna, señala que la Auditoría Interna consiste en la evaluación periódica:

Del grado de eficacia, eficiencia y efectividad del sistema de control interno, implantado por las Unidades Académicas y Dependencias de la Universidad de Buenos Aires.

Del resultado de la gestión de la organización auditada, en cuanto al grado de eficacia, eficiencia, transparencia y economía que hayan exhibido, en el cumplimiento de los objetivos y metas presupuestadas, en la utilización de los recursos públicos y en la ejecución de sus tareas y actividades y en el cumplimiento de las normas legales y dentro de los lineamientos de la política de la Universidad.

De la eficacia y eficiencia de los procesos críticos tanto sustantivos como de apoyo que la Entidad auditada tiene en operación, observando las deficiencias e irregularidades, estableciendo sus causas, estimando sus efectos y recomendando las medidas correctivas necesarias. (p.9)

Comentario:

Según la Universidad de Buenos Aires señala que la Auditoría Interna tiene como su función ayudar a las instituciones educativas, debido a que su propósito es medir el grado de eficacia, eficiencia, transparencia y economía a través del sistema de control interno; asimismo, contribuye en el cumplimiento de los objetivos y metas trazadas, identificando los procesos críticos dando a conocer las causas y efectos y recomendando medidas correctivas a fin de evitar deficiencias e irregularidades. Asimismo, dentro de las

recomendaciones se establecen medidas preventivas y correctivas de control quedando en decisión de aplicación por la Alta Gerencia.

Para Ruben Oscar Rusenas (1999), en su libro Manual de Auditoría Interna y Operativa; menciona que el trabajo del departamento de Auditoría Interna está orientado a:

1. Determinar la adhesión o cumplimiento de las políticas, metas y objetivos. Evaluar las normas que realmente se aplican en la empresa para optimizar la obtención de los objetivos políticos fijados.

2. Determinar la confiabilidad o seguridad de la información que es fuente para la toma de decisiones.

3. Asesorar a la dirección Superior. Cubrir las necesidades de asesoramiento técnico en función de sus conocimientos.

4. Salvaguardar el patrimonio de la empresa, ya fueren tanto los bienes materiales, como el medio humano que actúa en la misma.
5. Estudiar las posibilidades de fraude o robo, del patrimonio de la empresa y establecer las medidas que minimicen el riesgo.

6. Tratar de descubrir e informar de inmediato cuando detecte irregularidades, desviaciones o maniobras ilícitas.

7. Examinar, evaluar e informar sobre el sistema de control interno, el rendimiento de la organización y el estado en que ésta trata de lograr eficiencia y efectividad.

8. Sugerir y recomendar mejoras en cuanto al sistema de control interno, los sistemas administrativos y contables y todos los

procedimientos en general reduciendo los problemas de las auditorías anuales.

9. Colaborar con la auditoría externa realizando tareas de coordinación con la misma, para asegurar un adecuado control y revisión de la empresa.

La Auditoría Interna es una actividad independiente y objetiva de aseguramiento y consulta, cuya finalidad es aumentar el valor y mejorar las operaciones de la organización. Ayuda a que la organización cumpla con sus objetivos mediante la aplicación de un enfoque sistemático y disciplinado para evaluar y mejorar la efectividad de los procesos de manejo de riesgos, control y dirección. Dentro de los principales cambios en la nueva definición de Auditoría Interna, se resaltan:

1. Reconocimiento de que la Auditoría Interna es una función de consultoría y asesoramiento.
2. Énfasis en la necesidad de que la Auditoría Interna agregue valor a la organización.
3. Énfasis en la evaluación de los procesos de riesgos, controles y dirección para mejorar su efectividad. (p.79)

Comentario:

Por ello, Ruben Rusenas hace hincapié que el Departamento de Auditoría Interna es un órgano de control que contribuye en generar un entorno económico transparente y confiable de las operaciones, la cual promueve la salvaguarda del patrimonio de las empresas, que implica los bienes tangibles y el capital humano; que de acuerdo a las políticas y procedimientos establecidos por la Alta Dirección, se examina y se propone medidas que minimicen el riesgo y genera sinergias con los auditores externos, a fin de

asegurar el cumplimiento de los objetivos organizacionales de la empresa.

Del mismo modo, James Cashin, Paul Neuwirth y John Levy (1985) en el libro Manual de Auditoría definen a la Auditoría Interna es una actividad profesional, que implica el ejercicio de técnicas especializadas y la aceptación de una responsabilidad pública. Como profesional el Auditor desempeña sus labores mediante la aplicación de una serie de conocimientos especializados que vienen a formar el cuerpo técnico de su actividad; sin embargo, en el desempeño de su labor, el auditor adquiere responsabilidad, no solamente con la persona que contrata sus servicios, sino con un sinnúmero de personas que se encuentran relacionados directa e indirectamente con las del negocio.

Además, la Auditoría Interna cumple un rol muy importante en el gobierno corporativo; dicho gobierno es todo lo relacionado con las formas en que las corporaciones modernas son dirigidas y controladas, teniendo como objetivos:
Atraer capitales; Asegurar el buen manejo y administración de sociedades; Proteger los derechos de los inversionistas; Fomentar la confianza de los mercados financieros; Promover la competitividad. (p.122)

Comentario:
Según los autores James Cashin, Paul Neuwirth y John Levy señalan que el auditor interno cumple una labor de vital importancia en las organizaciones, debido a que su función de aseguramiento de los controles, transmite confianza a los interesados dentro de la empresa como fuera (stakeholders) de ella y por consiguiente, genera desarrollo, crecimiento y resultados financieros; asimismo, la participación del Auditor en el gobierno corporativo cumple un papel importante porque con sus recomendaciones promueve el

ejercicio de la ética y los valores apropiados en las organizaciones informando al Consejo de Administración.

Del mismo modo, para la Editorial Océano (2011) en su obra titulada Enciclopedia de la Auditoría Interna, la Auditoría Interna especialmente se aplica en el examen del sistema de control interno de las instituciones; en este sentido la auditoría del control interno es la evaluación de los sistemas de contabilidad y de control interno de una entidad, con el propósito de determinar la calidad de los mismos, el nivel de confianza que se les puede otorgar y si son eficaces y eficientes en el cumplimiento de sus objetivos. (p.46)

Comentario:

Según a lo indicado, por la Editorial Océano la Auditoría Interna es el proceso de obtener y evaluar objetivamente, en un período determinado, evidencia relativa a la información financiera, al comportamiento económico y al manejo de una entidad, con el propósito de informar sobre el grado de correspondencia entre aquéllos y los criterios o indicadores establecidos o los comportamientos generalizados. Su alcance implica la ejecución de un trabajo integral que abarca la revisión y análisis de la información financiera, de cumplimiento, de control interno y de gestión, dando como resultado una información valiosa para la toma de decisiones de la Alta Gerencia.

Para el Instituto Latinoamericano de Ciencias Fiscalizadoras (1981) en su libro Auditoría Interna; señala que el objetivo principal de la Auditoría Interna es ayudar a la administración de las entidades a alcanzar sus metas, con información, análisis, apreciaciones y recomendaciones relacionadas con las obligaciones y objetivos de su gestión.

La Auditoría Interna es una función de asesoría, no de línea. Por lo tanto, el auditor interno no debe ser autorizado para efectuar cambios en los procedimientos u operaciones de la entidad, ni para ordenar que éstos se efectúen. Su trabajo consiste en hacer análisis, revisiones y evaluaciones independientes y objetivos de los procedimientos y actividades existentes; informar acerca de la situación encontrada; y cuando lo juzgue necesario, recomendar cambios u otras medidas que sean tomadas en consideración por los funcionarios encargados de la administración y de las operaciones.

Un auditor interno no debe tener responsabilidades por operaciones específicas. Más bien, debe de ocuparse principalmente del rendimiento de otras personas, mantenerse independiente en todas sus labores, y prestar especial atención a los asuntos que requieren medidas correctivas. Su deber es presentar opiniones y sugerencias en forma constructiva, de manera que se estimulen las acciones de otras personas.

La Administración resulta beneficiada, asimismo, a través de una información oportuna sobre los problemas que pueden solucionarse a fin de mejorar el funcionamiento de la entidad. Estos, problemas, una vez examinados y evaluados, a menudo brindan la oportunidad de lograr costos menores, mayor eficiencia, y un modo más rápido de efectuar logros. (p.6)

Comentario:

Según Instituto Latinoamericano de Ciencias Fiscalizadoras señala que la actividad de Auditoría Interna ha pasado a ocupar un importante papel en las empresas, debido a que al analizar, revisar y evaluar las operaciones de las empresas, aporta una opinión razonable e independiente sobre el cumplimiento de los objetivos y metas previstos en la organización, apoyando la labor gerencial

mediante recomendaciones con acciones preventivas y correctivas para que sean consideraras y evaluadas por la Administración.

Del mismo modo, los autores Carmen Tapia, Rahell Rueda de Leon y Ricardo Silva (2017) en su libro Auditoría Interna Perspectivas de vanguardia; indican que la función de la Auditoría Interna es para todo tipo de organización, ya sea privada o pública, y cuya esencia es coadyuvar a que la dirección de las organizaciones a fin de lograr los objetivos planteados.

La Auditoría constituye una herramienta de control y supervisión que contribuye a la creación de una cultura de la disciplina de la organización, y permite descubrir fallas en las estructuras o vulnerabilidades existentes en la organización.

Además, la Auditoría Interna es una sola función practicada internamente por el propio personal de la empresa o también bajo la modalidad de outsourcing del departamento de Auditoría Interna. Es la entidad con diferentes enfoques de intervención y alcance, dado origen a los diferentes tipos de Auditoría que se puede aplicar.

En la actualidad, la planeación de una Auditoría Interna tiene que ser basada en los riesgos de la organización. Elaborar un plan anual de Auditoría es un reto importante para los auditores, así como fortalecer las relaciones con los stakeholders.

Tradicionalmente esta labor consistía en identificar unidades organizacionales con mayor impacto según el valor o volumen de transacciones en los estados financieros o de acuerdo con las apreciaciones de los auditores. Actualmente, diseñar un plan anual de Auditoría se debe centralizar en aquellas áreas de negocios o

procesos significativos respecto al tipo de riesgo que enfrenta la empresa, así como deberá tomar en cuenta otros elementos:

- La capacidad operativa y las competencias del equipo de auditores para el tema seleccionado para auditar.

- Complejidad de la materia a auditar y la oportunidad en la obtención de la información.

- Precisión respecto al énfasis que tendrá la revisión con base en los objetivos de control interno (operaciones, fiabilidad de reportes y cumplimiento).

- Cantidad de unidades o procesos que conforman el universo de la materia auditable de la organización.

No obstante, antes de decir el alcance de las revisiones a efectuar, se debe considerar que el área de Auditoría dispone de recursos limitados y, por consiguiente, es imposible auditar todo el universo auditable en un año, es por ello que ya hay algunas organizaciones que están haciendo planes bianuales. Asimismo, existen algunas empresas en las que las áreas de control interno y Auditoría externa trabajan en conjunto, de forma tal que se les permita tomar como base los esfuerzos que, en alguna revisión, haya efectuado para no duplicar y así profundizar en algún aspecto, según lo requieran. (p.8)

Comentario:

Según los autores Carmen Tapia, Rahell Rueda de Leon y Ricardo Silva señalan que la Auditoría Interna es un herramienta de control y supervisión que contribuye en concientizar a las áreas en identificar las fallas y vulnerabilidades en sus procesos internos además, el planeamiento anual de su labor es realizado basándose en los riesgos que enfrenta la organización, dando prioridad a las

áreas de negocios y los procesos significativos de acuerdo a los riesgos que se encuentran expuestos y de mayor impacto. Es importante señalar, que los recursos del Área de Auditoría Interna son limitados; por lo que, es imposible auditar toda una empresa en un año; teniendo en cuenta esta situación, es necesario elaborar un plan de auditoría de acuerdo a las prioridades de la Administración.

Para el autor Rodrigo Estupiñan (2015) en su libro Administración de Riesgos ERM y la Auditoría Interna; señala que en el sector privado, la existencia de un departamento de Auditoría Interna, debe estar establecida dentro de los estatutos de la Entidad o Empresa, bajo la denominación de Servicios de Aseguramiento en funciones y dependencia claramente indicados. En el sector oficial o público, deberá existir una Ley especifica que la determine, igualmente bajo funciones específicas y dependencia claramente identificadas, regularmente con dependencia directa al jefe de la Dependencia Pública.

La Auditoría Interna revisa la confiabilidad e integridad de la información, el cumplimiento con políticas y reglamentos, la salvaguarda de los activos, el uso económico y eficiente de los recursos, las metas y objetivos operativos establecidos. Los trabajos de Auditoría Interna abarcar todas las actividades financieras y de operaciones incluyendo sistemas, producción, ingeniería, comercialización y recursos humanos. (p.42)

Comentario:

Según lo indicado por Rodrigo Estupiñan, el ámbito de aplicación de la Auditoría Interna se da tanto en el sector público como privado cada una con características diferentes en la asignación de sus funciones y responsabilidades en el sector público se basa de mediante una ley aprobada esta debe regir en el departamento de auditoría y en el sector privado se establece mediante la

elaboración de un estatuto aprobado por la Alta Dirección; asimismo, señala que la Auditoría Interna tiene un como principal encargo el de velar el cumplimiento de las políticas y reglamentos, así como, la salvaguarda de activos, teniendo como alcance de revisión todas las áreas de la empresa.

Para Vicente Montesinos (1992) en su libro La Auditoría en España; menciona que la Auditoría Interna se empezó a desarrollar debido a la continua expansión que sufrían los negocios, ya que ésta añadía más información a suministrar a la dirección y por tanto el ejercicio de control sobre las operaciones se hacía más complicado. Problemas de descentralización, de incremento de operaciones rutinarias, de dispersión geográfica, de fusiones y adquisiciones, de incorporación de nuevas tecnologías o de diversificación de productos, entre otros, han puesto por sí mismos serios retos al control de la dirección.

Estos hechos han llevado inevitablemente a la delegación de responsabilidad y autoridad en el organigrama empresarial. Pero con esta asignación de funciones no concluye la responsabilidad de la dirección, ya que no puede delegar su responsabilidad general, por tanto tuvo que encauzar el control a través de verdaderos especialistas, y es en este punto cuando surge la necesidad de la Auditoría Interna con el fin de mantener la vigilancia sobre la cadena de control de la dirección.

El objetivo de la Auditoría Interna es el de servir de apoyo a todos los miembros de la dirección suministrándoles los análisis, evaluaciones, recomendaciones y comentarios oportunos concernientes a las operaciones que se han revisado, para que de esta forma puedan llevar a cabo un desempeño más efectivo de sus obligaciones.

Para el logro de este objetivo es necesario un programa sistemático de revisión y valoración con el fin de comprobar que las responsabilidades que se han delegado han sido bien encauzadas y que las políticas y procedimientos prefijados se han desarrollado como estaba previsto.

Es evidente por tanto que el asegurar la integridad del control y de la información, vendrá dado en la medida que existan revisiones regulares para determinar que el sistema de control es operativamente efectivo, ya que de lo contrario, por una parte, la dirección no tendría una fiabilidad total de las cuentas anuales y de los informes internos, cuando sean utilizados para la toma de decisiones y por otra el auditor externo no podría confiar en el sistema de control interno, a no ser que incrementase sus evidencias y la extensión de los procedimientos. (p.275)

Comentario:

Según lo señalado por Vicente Montesinos, la Auditoría Interna surge por la necesidad del crecimiento de las empresas y por tanto el control se hace más complicado es en donde la Auditoría Interna cumple una labor importante en el mantener la vigilancia sobre la cadena de control mediante una comunicación permanente a la dirección, siendo un apoyo a los accionistas proveyendo de análisis y recomendaciones, fortaleciendo el sistema de control interno y contribuye a la adecuada toma de decisiones de la Gerencia.

Para Marco Antonio Argandoña (2010), en el libro Nuevo enfoque de la auditoría Financiera, Presupuestal e interna, indica que en la actualidad la Auditoría Interna constituye un amplio examen de la empresa o institución referido a sus planes y objetivos, métodos y controles, significación operacional y utilización de los recursos humanos y físicos.

Los auditores internos deben conocer que en su desempeño tienen la obligación de regirse por el código de ética profesional que al efecto de la profesión se dicte por la sociedad. La experiencia ha demostrado que la adherencia a las normas más elevadas que se puedan establecer no es suficiente por sí misma.

El público debe asociar la imagen del auditor con la de una “moral más alta de lo normal,” por esa razón el auditor nunca debe permitir que sus intereses personales entren en conflicto con los de sus clientes, por otro lado, el auditor no debe realizar actos inmorales o ilegales que puedan dañar el prestigio de la profesión.

La ética general, comprende las normas mediante las cuales un individuo decide su conducta. Por lo general se consideran exigencias impuestas por la sociedad, los deberes morales y los efectos de las propias acciones.

El conocimiento y cumplimiento del código de ética por el auditor es fundamental y representa mucho más que una declaración de responsabilidad, constituye una herramienta de trabajo. A través de su cumplimiento el auditor declara al público que su profesión está interesada en proteger sus intereses y beneficiar a la sociedad ya que en esta profesión se necesita la confianza no sólo en la habilidad técnica del auditor sino también en su integridad.

El trabajo del auditor interno no tendrá ningún valor si los miembros de la organización a la que pertenece, no tienen fe en sus informes y no dudan en aceptarlos. En este marco, es un imperativo el cumplimiento de las normas de Auditoría Interna porque tienen relación estrecha con las Normas de auditoría generalmente aceptadas (NAGAS) siguientes:

1. Normas sobre Atributos: trata sobre los atributos que deben tener los auditores internos para que realicen sus funciones e informen de manera adecuada y eficaz a la autoridad facultada dentro de las organizaciones a las que pertenecen: Independencia y objetividad; Capacidad profesional; Debido cuidado profesional; Aseguramiento de la calidad.

2. Normas sobre Desempeño: estas describen la naturaleza de las actividades de Auditoría Interna y proveen criterios de calidad contra los cuales puede medirse la práctica de estos servicios: Planeamiento; Supervisión y revisión; Leyes y demás disposiciones legales; Calidad de la evidencia; Gestión de riesgos; Control Interno; Apoyo a la dirección estratégica.

3. Normas de Información: estas normas establecen los criterios para la presentación de los informes elaborados como resultado de los servicios de consultoría y de auditoría: Forma y contenido. (Instituto Auditores Internos de España, 2010).

   Por otro lado, las Normas internacionales de auditoría (NIAS) son las encargadas de la calidad en el desempeño del trabajo del auditor. Y se puede mencionar las siguientes:

   100-199 Asuntos Introductorios

   100 Prefacio a las Normas Internacionales de Auditoría
   El propósito de este prefacio es facilitar la comprensión de los objetivos y procedimientos operativos del Comité Internacional de Prácticas de Auditoría (IAPC), un comité permanente del Consejo de la Federación Internacional de Contadores Públicos, y el alcance y autoridad de los documentos que emite.

   110 Glosario de términos

Esta norma presenta un glosario de los términos de auditoría más comúnmente utilizados en estas normas internacionales.

120 Marco de referencia de las Normas Internacionales de Auditoría Esta norma describe el marco en el cual se emiten las Normas Internacionales de Auditoría con relación a los servicios que los auditores pueden brindar, comprende los informes financieros y los servicios de auditoría y relacionados. Este marco no es aplicable a otros servicios, tales como impuestos, consultoría y asesoramiento financiero y contable.

200-299 Responsabilidades

200 Objetivos y principios básicos que regulan una auditoría de estados financieros

Esta norma establece que el objetivo de la auditoría de estados financieros, preparados dentro del marco de políticas contables reconocidas, es permitir que el auditor exprese su opinión sobre dichos estados financieros para ayudar a establecer la credibilidad de los mismos. El auditor por lo general determina el alcance de auditoría de acuerdo con los requerimientos de las leyes, reglamentaciones o de los organismos profesionales correspondientes.

210 Cartas para el acuerdo de los términos sobre un trabajo de auditoría

Esta norma proporciona pautas para la preparación de la carta de contratación, en la cual el auditor documenta y confirma la aceptación de un trabajo, el objetivo y alcance de la auditoría, el grado de su responsabilidad ante el cliente y el formato del informe a ser emitido. Si bien esta norma no requiere explícitamente que el auditor obtenga una carta de contratación, proporciona una

orientación con respecto a su preparación de tal manera que se presume su uso.

220 Control de calidad del trabajo de auditoría

Esta norma trata sobre el control de calidad que se relaciona con el trabajo delegado a un equipo de trabajo y con las políticas y procedimientos adoptados por un profesional para asegurar en forma razonable que todas las auditorías efectuadas están de acuerdo con los principios básicos que regulan la auditoría.

230 Documentación

Esta norma define “documentación” como los papeles de trabajo preparados u obtenidos por el auditor y conservados por él para ayudar a la planificación, realización, supervisión y revisión del trabajo de auditoría y que proporciona evidencia del trabajo efectuado para respaldar el dictamen emitido. Se refiere también al uso de papeles de trabajo y legajos estandarizados de su propiedad y custodia.

240 Fraude y error

Esta norma trata la responsabilidad del auditor para la detección de información significativamente errónea que resulte de fraude o error, al efectuar la auditoría de información financiera. Proporciona una guía con respecto a los procedimientos que debe aplicar el auditor cuando encuentra situaciones que son motivo de sospecha o cuando determina que ha ocurrido un fraude o error.

250 Consideración de las leyes y reglamentos en una auditoría de estados financieros

Esta norma tiene como objetivo establecer normas y pautas sobre la responsabilidad del auditor en la consideración de las leyes y reglamentaciones en una auditoría de estados financieros. Esta norma es aplicable a las auditorías de estados financieros pero no

a otros trabajos en los que se contrata al auditor para emitir un informe especial sobre el cumplimiento de reglamentaciones específicas.

300-399 Planificación

300 Planificación

Esta norma establece que el auditor debe documentar por escrito su plan general y un programa de auditoría que defina los procedimientos necesarios para implantar dicho plan.

310 Conocimiento del negocio

El propósito de esta norma es determinar qué se entiende por conocimiento del negocio, por qué es importante para el auditor y para el equipo de auditoría que trabajan en una asignación, por qué es relevante para todas las fases de una auditoría y cómo el auditor obtiene y utiliza ese conocimiento.

315 Identificación y valoración de los Riesgos de Incorrección Material Mediante el Conocimiento de la Entidad y de su entorno.

Abarca la responsabilidad del auditor en reconocer y valorar los riesgos de incorrección material en los estados financieros y en las afirmaciones, teniendo como eje principal el conocer la entidad en un entorno tanto interno como externo (factores sectoriales y normativos, la naturaleza de la entidad, su estructura sus políticas contables, control interno, etc.)

Entre los procedimientos de valoración de riesgo se podrán incluir indagaciones (ante la alta gerencia y otras personas de la entidad), procedimientos analíticos, observación e inspección. Para determinar si ésta es relevante para la identificación de los riesgos, del mismo modo, evaluará si la información obtenida de auditorías

anteriores es adecuada o requiere cambios que no afecten la auditoría actual.

320 La importancia relativa de la auditoría

Esta norma se refiere a la interrelación entre la significatividad y el riesgo en el proceso de auditoría. Identifica tres componentes distintos del riesgo de auditoría: riesgo inherente, riesgo de control y riesgo de detección. Tomando conciencia de la relación entre significatividad y riesgo, el auditor puede modificar sus procedimientos para mantener el riesgo de auditoría en un nivel aceptable.

402 Consideraciones de auditoría en entidades que utilizan organizaciones prestadoras de servicios.

Esta norma establece que el auditor debe obtener una comprensión adecuada de los sistemas contables y el control interno para planificar la auditoría y desarrollar un enfoque de auditoría efectivo. La entidad emisora de los estados financieros puede contratar los servicios de una organización que, por ejemplo, ejecuta transacciones y lleva la contabilidad o registro de las transacciones, y procesa los datos correspondientes. El auditor debe considerar de qué manera una organización prestadora de servicios afecta los sistemas contables y el control interno del cliente.

500-599 Evidencia de Auditoría

500 Evidencia de Auditoría

El propósito de esta norma es ampliar el principio básico relacionado con la evidencia de auditoría suficiente y adecuada que debe obtener el auditor para poder arribar a conclusiones

razonables en las que basar su opinión con respecto a la información financiera y los métodos para obtener dicha evidencia.

501 Evidencia de auditoría - Consideraciones adicionales para partidas específicas

El propósito de esta norma es proporcionar pautas relacionadas con la obtención de evidencia de auditoría a través de la observación de inventarios, confirmación de cuentas a cobrar e indagación referida a acciones judiciales, ya que en general se considera que estos procedimientos brindan la evidencia de auditoría más confiable con respecto a ciertas afirmaciones.

Además, esta norma contiene algunas consideraciones sobre procedimientos de auditoría diseñados con el fin de constituir una base razonable para concluir si las inversiones a largo plazo están contabilizadas de acuerdo con los principios de contabilidad aplicables.

505 – Confirmaciones externas

La norma trata sobre la evidencia de auditoría que se obtiene como una respuesta directa escrita de un tercero la parte confirmante al auditor, en papel o en un medio electrónico u otro medio. El objetivo del auditor cuando utiliza procedimientos de confirmación externa es diseñar y aplicar dichos procedimientos con el fin de obtener evidencia de auditoría relevante y fiable.

510 Trabajos iniciales - Balances de apertura

El propósito de esta norma es proporcionar pautas con respecto a los saldos iniciales en el caso de los estados financieros auditados por primera vez o cuando la auditoría del año anterior fue realizada por otros auditores.

520 Procedimientos analíticos

Esta norma proporciona pautas detalladas con respecto a la naturaleza, objetivos y oportunidad de los procedimientos de

revisión analítica. El término “procedimiento de revisión analítica” se utiliza para describir el análisis de las relaciones y tendencias, que incluyen la investigación resultante de la variación inusual de los ítems.

530 Muestreo de auditoría

Esta norma identifica los factores que el auditor debe tener en cuenta al elaborar y seleccionar su muestra de auditoría y al evaluar los resultados de dichos procedimientos. Se aplica tanto para el muestreo estadístico como para el no estadístico.

540 Auditoría de estimaciones contables

Esta norma reafirma que los auditores tienen la responsabilidad de evaluar la razonabilidad de las estimaciones de la gerencia. Primero, deben tener en cuenta los controles, procedimientos y métodos de la gerencia para evaluar si ellos brindan una información correcta, completa y relevante. Deben poner especial atención en evaluaciones que resulten sensibles a variaciones, que sean subjetivas o susceptibles de errores significativos.

550 Partes relacionadas

Esta norma proporciona pautas referidas a los procedimientos que el auditor debería aplicar para obtener evidencia de auditoría con respecto a la identificación de las partes vinculadas y la exposición de las operaciones con dichas partes.

560 Hechos posteriores

Esta norma no permite el uso de doble fecha en el informe del auditor. Cuando se emiten estados financieros modificados que reemplazan estados financieros sobre los cuales el auditor ha emitido su informe previamente, dicho auditor debe hacer referencia al informe reemplazado. En ese caso, el auditor puede limitar su examen al hecho que requirió y, en caso de hacerlo, debe hacer una manifestación de tal hecho en su nuevo informe.

570 Empresa en marcha

Esta norma proporciona pautas para los auditores cuando surgen dudas sobre la aplicabilidad del principio de empresa en marcha como base para la preparación de estados financieros.

580 Representaciones de la administración

Esta norma orienta al auditor respecto de la utilización de las representaciones de la gerencia como evidencia de auditoría, los procedimientos que debe aplicar evaluar y documentar dichas representaciones y las circunstancias en las que se deberá obtener una representación por escrito. Trata también sobre las situaciones en las que la gerencia se niega a proporcionar o confirmar representaciones sobre asuntos que el auditor considera necesario.

600-699 Uso del trabajo de otros

600 Uso del trabajo de otro auditor

Esta norma requiere que el auditor principal documente en sus papeles de trabajo los componentes examinados por otros auditores, su significatividad con respecto al conjunto, los nombres de otros auditores, los procedimientos aplicados y las conclusiones alcanzadas por el autor principal con respecto a dichos componentes. Requiere también que el auditor efectúe ciertos procedimientos además de informar al otro auditor sobre la confianza que depositará en la información entregada por él.

610 Uso del trabajo de auditoría interna

Esta norma proporciona pautas detalladas con respecto a qué procedimientos deben ser considerados por el auditor externo para evaluar el trabajo de un auditor interno con el fin de utilizar dicho trabajo.

620 Uso del trabajo de un experto

El propósito de esta norma es proporcionar pautas con respecto a la responsabilidad del auditor y los procedimientos que debe aplicar con relación a la utilización del trabajo de un especialista como evidencia de auditoría. Cubre la determinación de la necesidad de utilizar el trabajo de un especialista, las destrezas y competencia necesaria, la evaluación de su trabajo y la referencia al especialista en el informe del auditor.

700-799 Conclusiones y dictamen de auditoría

700 Dictamen del auditor sobre los estados financieros

El propósito de esta norma es proporcionar pautas a los auditores con respecto a la forma y contenido del informe del auditor en relación con la auditoría independiente de los estados financieros de cualquier entidad. Cubre los elementos básicos del informe del auditor, describe los distintos tipos de informes e incluye ejemplos de cada uno de ellos.

705 Opinión modificada en el informe emitido por un auditor independiente

Esta norma trata de la responsabilidad que tiene el auditor de emitir un informe adecuado en función de las circunstancias cuando, al formarse una opinión de conformidad con la NIA 700, concluya que es necesaria una opinión modificada sobre los estados financieros. Establece tres tipos de opinión modificada, denominadas: opinión con salvedades, opinión desfavorable (o adversa) y denegación (o abstención) de opinión.

720 Otra información en documentos que contienen estados financieros auditados

Esta norma orienta al auditor con respecto al análisis de otra información incluida en documentos que contienen estados financieros junto con el informe del auditor sobre los mismos, sobre la cual no está obligado a informar. Establece que el auditor debería leer la otra información para asegurarse de que sea consistente con los estados financieros y/o no incluya información significativamente errónea.

800-899 Áreas especializadas

800 Dictamen del auditor sobre trabajos de auditoría con propósitos especiales

Esta norma proporciona pautas para informes sobre temas tales como componentes de los estados financieros, cumplimiento de acuerdos contractuales y estados preparados de acuerdo con bases contables integrales diferentes de las NIAS o de normas locales, y estados financieros resumidos.

810 El examen de información financiera proyectada

Esta norma explica la responsabilidad del auditor al examinar información financiera prospectiva (como por ejemplo presupuesto y proyecciones) y los supuestos sobre los que están basados; da pautas sobre procedimientos deseables e inclusive ejemplos de informes.

DECLARACIONES INTERNACIONALES PARA LA PRÁCTICA DE AUDITORIA

1000 Procedimientos de confirmación inter-bancos

El propósito de esta Declaración es ayudar al auditor externo y a miembros de la gerencia del banco, tales como auditores internos o inspectores, en los procedimientos de confirmación interbancaria.

Esta guía contribuirá a la efectividad de estos procedimientos y a la eficiencia del procesamiento de respuestas.

1001 Ambiente de procesamiento electrónico de datos - Microcomputadores

El propósito de esta Declaración es ayudar al auditor en la aplicación de la norma 400 describiendo el sistema de micro computación usado en estaciones de trabajo individuales. Esta Declaración describe los efectos del microcomputador sobre el sistema contable y los controles internos relacionados y sobre los procedimientos de auditoría.

1002 Ambiente de procesamiento electrónico de datos- Sistemas de computadores “en línea”

Esta Declaración forma parte de una serie cuyo objeto es ayudar al auditor en la aplicación de la norma 400 mediante la descripción de los sistemas computarizados “en línea” y su efecto en el sistema contable y los controles internos relacionados y en los procedimientos de auditoría.

1003 Ambiente de procedimiento electrónico de datos- Sistemas de base de datos

Esta Declaración forma parte de una serie cuyo objeto es ayudar al auditor en la aplicación de la norma 400 mediante la descripción de los sistemas de base de datos y su efecto en el sistema contable y los controles internos relacionados y en los procedimientos de auditoría.

1004 Relación entre los supervisores bancarios y los auditores externos

Esta Declaración define las responsabilidades fundamentales de la gerencia, analiza las características esenciales de los roles de los supervisores y auditores, considera el alcance de la supervisión de

funciones, y sugiere un mecanismo para coordinar en forma más eficiente el cumplimiento de las tareas de supervisores y auditores.

1005 Consideraciones particulares para la auditoría de pequeñas empresas

El propósito de esta Declaración es asistir al auditor en la aplicación de las Normas Internacionales de Auditoría en las situaciones típicas que se presentan en las pequeñas empresas.

1006 Auditoría de bancos comerciales internacionales

El propósito de esta Declaración es proporcionar una guía adicional a los auditores mediante la ampliación e interpretación de pautas para la auditoría de bancos comerciales internacionales. Sin embargo, no pretende ser una lista exhaustiva de los procedimientos y prácticas utilizados en este tipo de auditoría.

1007 Comunicaciones con la administración

Esta Declaración considera la relación del auditor con la gerencia, resume ciertos temas ya contemplados en las Normas Internacionales de Auditoría y brinda pautas adicionales. Algunos aspectos de la relación del auditor con la gerencia son determinados por requisitos legales y profesionales. Otros se rigen por los procedimientos y prácticas internas del auditor.

Los auditores deben tener en cuenta estos requisitos, procedimientos y prácticas. A los fines de esta Declaración, el término “gerencia” comprende a los funcionarios (ejecutivos de la administración que desempeñan funciones gerenciales jerárquicas). La gerencia sólo incluye a los directores y el comité de auditoría en aquellos casos en los que éstos desempeñan dichas funciones.

1008 Evaluación de riesgos y control interno- Características y consideraciones en un ambiente de procesamiento electrónico de datos (PED).
Esta Declaración contiene las características y consideraciones más importantes del ambiente PED: estructura organizativa, naturaleza del procesamiento, aspectos de diseño y procesamientos, controles internos, controles generales PED, controles de aplicación PED, revisión y evaluación de los controles generales y de aplicación PED.

1009 Técnicas de auditoría con ayuda de computadora
Esta Declaración es una ampliación de la norma 401 y proporciona pautas detalladas con respecto al uso de técnicas de auditoría asistidas por la computadora.

Por otro lado las Normas para el Ejercicio Profesional de la Auditoría Interna Las Normas para el Ejercicio Profesional de la Auditoría Interna, elaboradas por el Instituto de Auditores Internos, que define los principios básicos que representan el ejercicio de la Auditoría Interna y provee un marco internacional para ejercer y promover un amplio rango de sus actividades de valor agregado.

Para el cumplimiento de estos propósitos, las normas requieren que los auditores internos tengan entre sus atributos el ser independientes y objetivos para el cumplimiento de su trabajo. Al respecto, señalan:

Normas sobre Independencia y Objetividad

1100 – Independencia y Objetividad
La actividad de Auditoría Interna debe ser independiente, y los auditores internos deben ser objetivos en el cumplimiento de su trabajo.

1110 – Independencia de la Organización

El director ejecutivo de auditoría debe responder ante un nivel jerárquico tal dentro de la organización que permita a la actividad de auditoría interna cumplir con sus responsabilidades.

1110.A1 – La actividad de Auditoría Interna debe estar libre de injerencias al determinar el alcance de Auditoría Interna, al desempeñar su trabajo y al comunicar sus resultados.

1120 – Objetividad Individual

Los auditores internos deben tener una actitud imparcial y neutral, y evitar conflictos de intereses.

1130 – Impedimentos a la Independencia u Objetividad

Si la independencia u objetividad se viese comprometida de hecho o en apariencia, los detalles del impedimento deben darse a conocer a las partes correspondientes. La naturaleza de esta comunicación dependerá del impedimento.

1130.A1 – Los auditores internos deben abstenerse de evaluar operaciones específicas de las cuales hayan sido previamente responsables. Se presume que hay impedimento de objetividad si un auditor provee servicios de aseguramiento para una actividad de la cual el mismo haya tenido responsabilidades en el año inmediato anterior.

1130.A2 – Los trabajos de aseguramiento para funciones por las cuales el director ejecutivo de auditoría tiene responsabilidades deben ser supervisadas por alguien fuera de la actividad de Auditoría Interna.

1130.C1 – Los auditores internos pueden proporcionar servicios de consultoría relacionados a operaciones de las cuales hayan sido previamente responsables.

1130.C2 – Si los auditores internos tuvieran impedimentos potenciales a la independencia u objetividad relacionados con servicios de consultoría que les hayan sido propuestos, deberá declararse esta situación al cliente antes de aceptar el trabajo.
(p.119)

Comentario:
Señala que en el desempeño de sus funciones de los auditores internos deben regirse mediante el código de ética profesional donde se establece los principios y reglas de conducta que gobiernan a los profesionales en el ejercicio de la Auditoría Interna dentro de una empresa u organización; asimismo, como parte del proceso de la auditoría debe basarse de las Normas de Auditoría Generalmente Aceptadas (NAGAS), el cumplimiento de estas normas garantiza la calidad del trabajo profesional del auditor, mediante las normas comprende la medición de los procedimientos que van de ser ejecutados y los objetivos alcanzados; asimismo, el juicio del auditor que se plasma en un informe de hallazgos y recomendaciones.

RESEÑA HISTORCA - GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Desde tiempos inmemorables el hombre ha resguardado y protegido con celo sus conocimientos debido a la ventaja y poder que éste le producía sobre otros hombres o sociedades. En la antigüedad surgen las bibliotecas, lugares donde se podía resguardar la información para trasmitirla y para evitar que otros la

obtuvieran, dando así algunas de las primeras muestras de protección de la información.

Sun Tzuen en “El arte de la guerra” y Nicolás Maquiavelo en “El Príncipe” señalan la importancia de la información sobre los adversarios y el cabal conocimiento de sus propósitos para la toma de decisiones. Durante la Segunda Guerra Mundial se crean la mayoría de los servicios de inteligencia del mundo con el fin de obtener información valiosa e influyente, creándose grandes redes de espionaje.

Como forma de protección surge la contrainteligencia. Con el devenir de los años al incrementarse el alcance de la tecnología, el cuidado dela información se ha vuelto crucial para los hombres, las organizaciones y las sociedades.

Sin dudas uno de los pioneros en el tema fue James P. Anderson, quien allá por 1980 y a pedido de un ente gubernamental produjo uno de los primeros escritos relacionados con el tema, y es allí donde se sientan también las bases de palabras que hoy suenan como naturales, pero que por aquella época parecían ciencia ficción. Lo más importante de este documento es que James Anderson da una definición de los principales agentes de las amenazas informáticas.

Entre sus definiciones se encuentran términos base de la seguridad informática como Ataque o Vulnerabilidad. En la definición de Vulnerabilidad hacer referencia a “una falla conocida o sospecha, tanto en hardware como en el diseño de software, o la operación de un sistema que se expone a la penetración de sus información con exposición accidental”. En cuanto al Ataque, lo define como “una formulación especifica o ejecución de un plan para lleva a cabo una

amenaza". Siendo que la seguridad de la información es un derecho y una obligación de todos.

Durante los años 80 y principios de los 90 la Seguridad Informática se centraba en proteger los equipos de los usuarios, es decir, proporcionar seguridad a los ordenadores y su sistema operativo. Esta seguridad lógica, entendida como la seguridad de los equipos informáticos para evitar que dejasen de funcionar correctamente, se centraba en la protección contra virus informáticos.

Con la aparición de Internet y su uso globalizado a nivel empresarial la Seguridad Informática comenzó a enfocarse hacia la conectividad de redes o networking, protegiendo los equipos servidores de aplicaciones informáticas, y los equipos servidores accesibles públicamente a través de Internet, y controlando la seguridad a nivel periférico a través de dispositivos como Firewalls. Es decir, la posibilidad tecnológica de "estar conectados" llevaba implícita la aparición de nuevas vulnerabilidades que podían ser explotadas, la exposición de información crucial para el negocio que podía ser accesible precisamente gracias a esa conectividad.

La evolución de seguridad de la Información es un concepto más global que persigue definir e integrar Políticas de Seguridad en los planes estratégicos. Se cuantifican los riesgos, se identifican aquellos más críticos para el negocio de forma continua, se plantean escenarios de crisis y se diseñan planes de continuidad de negocio y recuperación ante desastres.

Toda esta información, junto con un buen diseño del organigrama de seguridad, una profunda integración de la seguridad en los planes estratégicos de la empresa, y una permanente implicación de la gerencia y del personal directivo de la empresa, permitirán conocer dónde y cómo utilizar las medidas técnicas de Seguridad

Informática (línea operativa) en el marco de la Seguridad de la Información y sus medidas organizativas (línea estratégica).

2.2.2 VARIABLE DEPENDIENTE
Y: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Para Godoy Lemus (2014) en su revista de la Segunda Corte Del Doctorado En Seguridad Estratégica, define a la seguridad de la información como el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos. Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

El campo de la seguridad de la información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial. Este campo ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, planificación de la continuidad del negocio, ciencia forense digital y administración de sistemas de gestión de seguridad, entre otros.

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos de saber que puede ser confidencial: la información está centralizada y puede

tener un alto valor. Puede ser divulgada, mal utilizada, ser robada, borrada o saboteada. Esto afecta su disponibilidad y la pone en riesgo. La información es poder, y según las posibilidades estratégicas que ofrece tener acceso a cierta información, ésta se clasifica como:

Crítica : Es indispensable para la operación de la empresa.
Valiosa : Es un activo de la empresa y muy valioso.
Sensible : Debe de ser conocida por las personas autorizadas

Existen dos palabras muy importantes que son riesgo y seguridad:

Riesgo: Es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones de negocio.

Seguridad: Es una forma de protección contra los riesgos.

La seguridad de la información comprende diversos aspectos entre ellos la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, recuperación de los riesgos.

Precisamente la reducción o eliminación de riesgos asociado a una cierta información es el objeto de la seguridad de la información y la seguridad informática.

Más concretamente, la seguridad de la información tiene como objeto los sistemas el acceso, uso, divulgación, interrupción o destrucción no autorizada de información. Los términos seguridad de la información, seguridad informática y garantía de la información son usados frecuentemente como sinónimos porque

todos ellos persiguen una misma finalidad al proteger la confidencialidad, integridad y disponibilidad de la información. Sin embargo, no son exactamente lo mismo existiendo algunas diferencias sutiles.

Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración. Además, la seguridad de la información involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial.

Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran. La seguridad de la información incumbe a gobiernos, entidades militares, instituciones financieras, los hospitales y las empresas privadas con información confidencial sobre sus empleados, clientes, productos, investigación y su situación financiera.

En caso de que la información confidencial de una empresa, sus clientes, sus decisiones, su estado financiero o nueva línea de productos caigan en manos de un competidor; se vuelva pública de forma no autorizada, podría ser causa de la pérdida de credibilidad de los clientes, pérdida de negocios, demandas legales o incluso la quiebra de la misma.

Por más de veinte años la Seguridad de la Información ha declarado que la confidencialidad, integridad y disponibilidad (conocida como la Tríada CIA, del inglés: "Confidentiality, Integrity,

Availability") son los principios básicos de la seguridad de la información.

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, si alguna de estas características falla no estamos ante nada seguro.

Es preciso anotar, además, que la seguridad no es ningún hito, es más bien un proceso continuo que hay que gestionar conociendo siempre las vulnerabilidades y las amenazas que se ciñen sobre cualquier información, teniendo siempre en cuenta las causas de riesgo y la probabilidad de que ocurran, así como el impacto que puede tener. Una vez conocidos todos estos puntos, y nunca antes, deberán tomarse las medidas de seguridad oportunas.

A. Confidencialidad

Es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y el comerciante de a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se publica información privada, cuando un laptop con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad.
Integridad

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) Grosso modo, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital Es uno de los pilares fundamentales de la seguridad de la información

B. Disponibilidad

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Grosso modo, la disponibilidad es el acceso a la información y a los

sistemas por personas autorizadas en el momento que así lo requieran.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La Alta disponibilidad sistemas objetivo debe estar disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

Garantizar la disponibilidad implica también la prevención de ataque de denegación de servicio. Para poder manejar con mayor facilidad la seguridad de la información, las empresas o negocios se pueden ayudar con un sistema de gestión que permita conocer, administrar y minimizar los posibles riesgos que atenten contra la seguridad de la información del negocio.

La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requiera. Tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de web etc, mediante el uso de clusters o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar.

C. Autenticación o autentificación

Es la propiedad que permite identificar el generador de la información. Por ejemplo al recibir un mensaje de alguien, estar seguro que es de ese alguien el que lo ha mandado, y no una tercera persona haciéndose pasar por la otra (suplantación de identidad). En un sistema informático se suele conseguir este factor con el uso de cuentas de usuario y contraseñas de acceso. (p.162)

Comentario:

Según Rodolfo Godoy señala que la Seguridad de la Información tiene como finalidad proteger de la información sensible y de los sistemas de la información estableciendo controles en el adecuado acceso, uso, divulgación dentro de una organización. Teniendo en cuenta que la seguridad de la información puede estar libre de peligro o daño y pueda afectar el funcionamiento de las empresas, tanto económico y reputacional, considerando que para una correcta gestión de la información se debe de aplicar los principios básicos de la seguridad de información que son: Confidencialidad, Integridad, Disponibilidad, Autenticación o Autentificación.

Para Aguilera Lopez, Purificación en su libro Seguridad Informática (2010) la seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable. Un sistema de información, no obstante a las medidas de seguridad que se le apliquen, no deja de tener siempre un margen de riesgo.

Para afrontar el establecimiento de un sistema de seguridad es necesario conocer:

- Cuáles son los elementos que componen el sistema. Esta información se obtiene mediante entrevistas con los responsables o directivos de la organización para la que se hace el estudio de riesgos y mediante apreciación directa.

- Cuáles son los peligros que afectan al sistema, accidentales o provocados. Se deducen tanto de los datos aportados por la organización como por el estudio directo del sistema mediante la realización de pruebas y muestreos sobre el mismo.

- Cuáles son las medidas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos potenciales. Se trata de decidir cuáles serán los servicios y mecanismos de seguridad que reducirían los riesgos al máximo posible.

Tras el estudio de riesgos y la implantación de medidas, debe hacerse un seguimiento periódico, revisando y actualizando las medidas adoptadas. Todos los elementos que participan en un sistema de información pueden verse afectados por fallos de seguridad, si bien se suele considerar la información como el factor más vulnerable.

El hardware y otros elementos físicos se pueden volver a comprar o restaurar, el software puede ser reinstalado, pero la información dañada no siempre es recuperable, lo que puede ocasionar daños de diversa índole sobre la economía y la imagen de la organización y, a veces, también causar perjuicios a personas. Otro aspecto a tener en cuenta es que la mayoría de los fallos de seguridad se deben al factor humano.

Los daños producidos por falta de seguridad pueden causar pérdidas económicas o de credibilidad y prestigio a una organización. Su origen puede ser:

• Fortuito. Errores cometidos accidentalmente por los usuarios, accidentes, cortes de fluido eléctrico, averías del sistema, catástrofes naturales, etc.

• Fraudulento. Daños causados por software malicioso, intrusos o por la mala voluntad de algún miembro del personal con acceso al sistema, robo o accidentes provocados.

Se considera seguro un sistema que cumple con las propiedades de integridad, confidencialidad y disponibilidad de la información. Cada una de estas propiedades conlleva la implantación de determinados servicios y mecanismos de seguridad:

Integridad

Este principio garantiza la autenticidad y precisión de la información sin importar el momento en que esta se solicita, o dicho de otra manera, una garantía de que los datos no han sido alterados ni destruidos de modo no autorizado.

Para evitar este tipo de riesgos se debe dotar al sistema de mecanismos que prevengan y detecten cuándo se produce un fallo de integridad y que puedan tratar y resolver los errores que se han descubierto.

Confidencialidad

La OCDE (Organización para la Cooperación y el Desarrollo Económico), en sus Directrices para la Seguridad de los Sistemas de Información define la confidencialidad como «el hecho de que los datos o informaciones estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada».

Para prevenir errores de confidencialidad debe diseñarse un control de accesos al sistema: quién puede acceder, a qué parte del sistema, en qué momento y para realizar qué tipo de operaciones.

Disponibilidad

La información ha de estar disponible para los usuarios autorizados cuando la necesiten. Se deben aplicar medidas que protejan la información, así como crear copias de seguridad y mecanismos para restaurar los datos que accidental o intencionadamente se hubiesen dañado o destruido.

Al analizar un sistema de información al que se pretende dotar de unas medidas de seguridad, hay que tener en cuenta los siguientes elementos: activos, amenazas, riesgos, vulnerabilidades, ataques e impactos.

Activos

Son los recursos que pertenecen al propio sistema de información o que están relacionados con este. La presencia de los activos facilita el funcionamiento de la empresa u organización y la consecución de sus objetivos. Al hacer un estudio de los activos existentes hay que tener en cuenta la relación que guardan entre ellos y la influencia que se ejercen: cómo afectaría en uno de ellos un daño ocurrido a otro.

Podemos clasificarlos en los siguientes tipos:

• Datos. Constituyen el núcleo de toda organización, hasta tal punto que se tiende a considerar que el resto de los activos están al servicio de la protección de los datos. Normalmente están organizados en bases de datos y almacenados en soportes de diferente tipo. El funcionamiento de una empresa u organización depende de sus datos, que pueden ser de todo tipo: económicos, fiscales, de recursos humanos, clientes o proveedores.

Cada tipo de dato merece un estudio independiente de riesgo por la repercusión que su deterioro o pérdida pueda causar, como por

ejemplo los relativos a la intimidad y honor de las personas u otros de índole confidencial.

• Software. Constituido por los sistemas operativos y el conjunto de aplicaciones instaladas en los equipos de un sistema de información que reciben y gestionan o transforman los datos para darles el fin que se tenga establecido.

• Hardware. Se trata de los equipos (servidores y terminales) que contienen las aplicaciones y permiten su funcionamiento, a la vez que almacenan los datos del sistema de información. Incluimos en este grupo los periféricos y elementos accesorios que sirven para asegurar el correcto funcionamiento de los equipos o servir de vía de transmisión de los datos (módem, router, instalación eléctrica o sistemas de alimentación ininterrumpida, destructores de soportes informáticos).

• Redes. Desde las redes locales de la propia organización hasta las metropolitanas o internet. Representan la vía de comunicación y transmisión de datos a distancia.

• Soportes. Los lugares en donde la información queda registrada y almacenada durante largos períodos o de forma permanente (DVD, CD, tarjetas de memoria, discos duros externos dedicados al almacenamiento, microfilms e incluso papel).

• Instalaciones. Son los lugares que albergan los sistemas de información y de comunicaciones. Normalmente se trata de oficinas, despachos, locales o edificios, pero también pueden ser vehículos y otros medios de desplazamiento.

• Personal. El conjunto de personas que interactúan con el sistema de información: administradores, programadores, usuarios internos

y externos y resto de personal de la empresa. Los estudios calculan que se producen más fallos de seguridad por intervención del factor humano que por fallos en la tecnología.

• Servicios que se ofrecen a clientes o usuarios: productos, servicios, sitios web, foros, correo electrónico y otros servicios de comunicaciones, información, seguridad, etc.

Amenazas

En sistemas de información se entiende por amenaza la presencia de uno o más factores de diversa índole (personas, máquinas o sucesos) que –de tener la oportunidad– atacarían al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad. Hay diferentes tipos de amenazas de las que hay que proteger al sistema, desde las físicas como cortes eléctricos, fallos del hardware o riesgos ambientales hasta los errores intencionados o no de los usuarios, la entrada de software malicioso (virus, troyanos, gusanos) o el robo, destrucción o modificación de la información.

En función del tipo de alteración, daño o intervención que podrían producir sobre la información, las amenazas se clasifican en cuatro grupos:

• De interrupción. El objetivo de la amenaza es deshabilitar el acceso a la información; por ejemplo, destruyendo componentes físicos como el disco duro, bloqueando el acceso a los datos, o cortando o saturando los canales de comunicación.

• De interceptación. Personas, programas o equipos no autorizados podrían acceder a un determinado recurso del sistema y captar información confidencial de la organización, como pueden ser datos, programas o identidad de personas.

• De modificación. Personas, programas o equipos no autorizados no solamente accederían a los programas y datos de un sistema de información sino que además los modificarían. Por ejemplo, modificar la respuesta enviada a un usuario conectado o alterar el comportamiento de una aplicación instalada.

Según su origen las amenazas se clasifican en:

• Accidentales. Accidentes meteorológicos, incendios, inundaciones, fallos en los equipos, en las redes, en los sistemas operativos o en el software, errores humanos.

• Intencionadas. Son debidas siempre a la acción humana, como la introducción de software malicioso –malware– (aunque este penetre en el sistema por algún procedimiento automático, su origen es siempre humano), intrusión informática (con frecuencia se produce previa la introducción de malware en los equipos), robos o hurtos. Las amenazas intencionadas pueden tener su origen en el exterior de la organización o incluso en el personal de la misma.

Riesgos

Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma.

Ante un determinado riesgo, una organización puede optar por tres alternativas distintas:

• Asumirlo sin hacer nada. Esto solamente resulta lógico cuando el perjuicio esperado no tiene valor alguno o cuando el coste de aplicación de medidas superaría al de la reparación del daño.

• Aplicar medidas para disminuirlo o anularlo.
• Transferirlo (por ejemplo, contratando un seguro).

Vulnerabilidades
Probabilidades que existen de que una amenaza se materialice contra un activo.

No todos los activos son vulnerables a las mismas amenazas. Por ejemplo, los datos son vulnerables a la acción de los hackers, mientras que una instalación eléctrica es vulnerable a un cortocircuito. Al hacer el análisis de riesgos hay que tener en cuenta la vulnerabilidad de cada activo.

Se dice que se ha producido un ataque accidental o deliberado contra el sistema cuando se ha materializado una amenaza. En función del impacto causado a los activos atacados, los ataques se clasifican en:

• Activos. Si modifican, dañan, suprimen o agregan información, o bien bloquean o saturan los canales de comunicación.

• Pasivos. Solamente acceden sin autorización a los datos contenidos en el sistema. Son los más difíciles de detectar.

Un ataque puede ser directo o indirecto, si se produce desde el atacante al elemento «víctima» directamente, o a través de recursos o personas intermediarias.

Proceso del análisis de riesgos: Para implantar una política de seguridad en un sistema de información es necesario seguir un esquema lógico.

- Hacer inventario y valoración de los activos.
- Identificar y valorar las amenazas que puedan afectar a la seguridad de los activos.

- Identificar y evaluar las medidas de seguridad existentes.
- Identificar y valorar las vulnerabilidades de los activos a las amenazas que les afectan.
- Identificar los objetivos de seguridad de la organización.
- Determinar sistemas de medición de riesgos.
- Determinar el impacto que produciría un ataque.
- Identificar y seleccionar las medidas de protección. (p.9)

Comentario:

Según Purificación Aguilera señala que la seguridad de la información cuenta con normas, procedimientos, métodos y técnicas para asegurar que la información de las empresas se encuentre a salvo, considerando la implementación de un sistema de seguridad que identifique los riesgos para poder establecer planes de contingencia ante posibles amenazas que puedan producir perdidas económicas, de credibilidad y prestigio; asimismo, se debe de clasificar los activos informáticos por el grado de daño que afectaría a la organización y estableciendo en el análisis de los riesgos las acciones para poder minimizar su materialización optando por tres alternativas: asumirlo sin hacer nada, aplicar medidas correctivas o transferirlo.

Del mismo modo, en la Guía de Auditoría de Tecnología Global del Instituto de Auditores Internos (2005) denominada Controles de Tecnología de Información, establece que la seguridad de la información es una parte fundamental de todos los controles de TI. La seguridad de la información se aplica desde la infraestructura hasta los datos y es la base para la fiabilidad de la mayoría de los otros controles de TI.

La Auditoría Interna es una parte esencial del proceso de gobierno corporativo, independientemente que si se utiliza un grupo de Auditoría Interna específico. Los auditores internos deben tener conocimiento y comprensión general de TI, pero el nivel de tal

conocimiento varía según la categoría de las auditorías o el nivel de supervisión (Norma del IIA 1210.A3). El IIA define tres categorías de conocimiento de TI para auditores internos que se describen en el Apéndice C. En relación con la TI, la función de la Auditoría Interna implica:

• Asesorar al comité de auditoría y a la alta dirección sobre aspectos relacionados con el control interno de TI.

• Asegurar que la TI se incluya en el universo de auditoría y en el plan anual (seleccionar temas).
• Asegurar que los riesgos de TI sean considerados cuando se asignan los recursos y las prioridades en las actividades de auditoría.

• Definir los recursos de TI necesarios para el departamento de auditoría, incluida la formación especializada del personal de auditoría.

• Asegurar que la planificación de auditoría considere los aspectos de TI en cada auditoría.

• Actuar como enlace con los clientes de auditoría para determinar qué desean o qué necesitan saber.

• Realizar análisis de riesgos de TI.
• Determinar qué constituye una evidencia fiable y verificable.
• Realizar auditorías de controles de TI a nivel de empresa.
• Realizar auditorías de los controles generales de TI.
• Realizar auditorías de los controles de aplicación.
• Realizar auditorías especializadas de los controles técnicos de TI.
• Utilizar de manera eficiente y eficaz la TI para contribuir al proceso de auditoría.

• Durante las actividades de desarrollo o análisis de sistemas, debe actuar como experto que conoce cómo se pueden implementar o eludir los controles.
• Ayudar en la supervisión y verificación de la adecuada implementación de actividades que minimicen todos los riesgos de TI conocidos y documentados.

Aprovechando el conocimiento de los riesgos de TI, el auditor puede validar la existencia de controles eficaces para alcanzar el grado de aceptación y tolerancia al riesgo de la organización en cuanto a TI. La evaluación del auditor incluirá los debates con los miembros de la dirección y en última instancia con el consejo. El nivel de detalle de esos debates puede ser determinado por el director de riesgos con la información aportada por el director de TI, el director de seguridad de la información, el director de seguridad, el DEA, y por los propietarios de los procesos. La decisión final respecto al grado de aceptación y tolerancia al riesgo debe ser tomada por el comité de riesgo con el asesoramiento del comité de auditoría, y debe ser apoyada por el consejo por completo. Las definiciones de grado de aceptación del riesgo y tolerancia deben ser comunicadas a todos los gestores relevantes para su efectiva implementación.

La separación de funciones es un elemento vital para muchos controles. La estructura de una organización no debe asignar la responsabilidad de todos los aspectos del procesamiento de datos a un solo individuo o departamento. Las funciones de iniciar, autorizar, ingresar, procesar y verificar datos se deben separar para garantizar que ningún individuo pueda realizar ambas funciones y crear un error, omisión, u otra irregularidad y autorizarlo y/o ocultar la evidencia. Los controles de separación de funciones en los sistemas de aplicación se proporcionan al otorgar privilegios de acceso sólo en función de los requerimientos del trabajo desempeñado para procesar funciones y ganar acceso a la información sensible.

La separación tradicional de funciones en el entorno de TI se divide entre desarrollo de sistemas y operaciones. El área de Operaciones y Explotación debe ser responsable de ejecutar los sistemas de producción, a excepción de la distribución de los cambios, y debe tener poco o ningún contacto con el proceso de desarrollo. Este control debe incluir restricciones que impidan el acceso de los operadores para modificar programas, sistemas o datos de producción. De igual manera, el personal de desarrollo de sistemas debe tener poco contacto con los sistemas en producción. Durante la implementación y los cambios de procesos, al asignar funciones específicas al personal responsable de los sistemas de aplicación y a los responsables de operaciones, se puede impulsar la correcta separación de funciones.

En organizaciones grandes, se deben considerar muchas otras funciones para asegurar la separación apropiada y esos controles pueden ser bastante detallados. Por ejemplo, las cuentas privilegiadas, como el grupo administrador de Windows y de superusuario en UNIX, pueden modificar registros de entrada, obtener acceso a cualquier archivo y en muchos casos actuar como cualquier usuario o función. Es importante restringir al mínimo el número de personas con este privilegio.

También hay herramientas de software disponibles que se deben considerar para limitar la capacidad de los usuarios con cuentas privilegiadas y para supervisar sus actividades. (p.17)

Comentarios:

Según la Guía de Auditoría de Tecnología Global del Instituto de Auditores Internos señala que la seguridad de la información parte desde la infraestructura que soporta la información hasta los datos que son utilizados por los usuarios finales; por lo que, el auditor debe

contar con un conocimiento y comprensión general de TI, a fin de considerar los recursos y prioridades en la actividad de la auditoría y evaluando de vital importancia la separación de funciones que comprende el inicio, autorización, ingreso, procesamiento y verificación de los datos a un solo usuario; de tal manera, se limite los usuarios con cuentas privilegias y se apliquen procedimientos de control.

Para los autores Maria Alegre y Alfonso Garcia-Cervigón (2011) en su libro Seguridad Informática, la seguridad informática se puede definir como un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información de un sistema informático e intentar reducir las amenazas que pueden afectar al mismo.

Dentro de la seguridad informática podemos encontrar elementos y técnicas tanto hardware, como software, así como dispositivos físicos y medios humanos. Actualmente existen un gran número de razones para aplicar y afianzar la seguridad informática.

En los sistemas informáticos actuales no existe el concepto de ordenador aislado como sucedía en ordenadores de generaciones anteriores a la actual, sino que es extraño un sistema informático que no esté dentro de una red de ordenadores para compartir recursos e información, así como acceso a Internet, con lo cual las amenazas les pueden llegar desde el interior, así como desde el exterior, y al estar conectados en red, un ataque a un equipo, puede afectar a todo el conjunto (p.2)

Comentarios:

Según lo indicado por los autores del libro, manifiestan la importancia de identificar los riesgos asociados la gestión de la seguridad de la información a fin de mejorar las operaciones y contar con sistemas

seguros, siendo su alcance en los equipos informáticos (hardware) y en la concientización del personal usuario; asimismo, destaca que las amenazas de afectar la información de las empresas actualmente el impacto sea mayor, debido a que las operaciones se encuentran en la red o en la Internet, esto conlleva a que un solo ataque pueda afectar en conjunto.

Para Javier Areitio (2008) en su libro Seguridad de la Informática indica que la seguridad de información es una disciplina en continua evolución. La meta final de la seguridad es permitir que una organización cumpla con todos sus objetivos de negocio o misión, implementando sistemas que tengan un especial cuidado y consideración hacia los riesgos relativos a las TIC (Tecnología de la Información y Comunicaciones) de la organización, a sus socios comerciales, clientes, administración pública, suministradores, etc (p.2).

Comentarios:

Según el libro Seguridad de la Informática considera que esta disciplina se somete a constantes cambios debido a diferentes razones, como la interconexión global con Internet, la complejidad masiva de los sistemas, la emisión de actualizaciones de las versiones de los softwares y el desarrollo evolutivo de los programas; asimismo, la implementación de una gestión de seguridad debe estar basada en monitorear los riesgos relacionados a las Tecnología de la Información y Comunicaciones.

2.3 DEFINICIONES CONCEPTUALES

2.3.1 X: AUDITORIA INTERNA

Spencer Pickett K.H. (2007). Según el autor en su libro titulado Manual Básico de Auditoría Interna señala que: Los retos del mundo actual que está en proceso de cambio ofrecen grandes oportunidades a la dirección de las empresas y al consejo de administración e indican la necesidad de una auditoría competente. Sobre todo en estos tiempos de cambios constantes, la Auditoría Interna es muy importante para las operaciones eficientes, para los controles internos eficientes y para la gestión de riesgos, para una gobernabilidad corporativa fuerte y, en algunos casos, para la propia supervivencia de la empresa. (p.502)

Comentario:

Según el autor Spencer Pickett (2007) considera que la Auditoría Interna cumple un papel importante en la toma de decisiones para la alta dirección basándose en el cumplimiento de las operaciones eficientes mediante la evaluación de los controles internos y una adecuada gestión de riesgos por ello, contribuye en vigilar y salvaguardar los bienes de las empresas; asimismo, destaca la necesidad en el mundo actual de contar con un área de Auditoría Interna, a fin de mantener su competitividad y continuidad de las empresas.

Borrajo Manuel (2002) en su artículo titulado “La Auditoría Interna y Externa” define como: La Auditoría Interna debe ser una función de control, de gestión y de consulta, adscrita al Comité de Auditoría, con la misión establecida por el Consejo de la Administración, de vigilancia y mantenimiento de un adecuado sistema de control interno y la prevención y valorización de los riesgos, que trabaja sometida al cumplimiento de las Normas para el Ejercicio Profesional de la Auditoría Interna del Instituto de Auditores

Internos. Hay una serie de condicionantes que la caracterizan, como son, la objetividad, la veracidad, la independencia, el cumplimiento de sus normas y la utilización de los métodos de auditoría interna. (p.51)

Comentario:

Según el autor Manuel Borrajo (2002) define a la Auditoría Interna como una función que vela por un adecuado sistema de control interno, prestando los servicios de control, gestión y de consulta al Consejo de Administración, desempañando su labor de acuerdo a los establecido a las Normas para el Ejercicio Profesional de la Auditoría del Instituto de Auditores Internos, haciendo que el alcance de la Auditoría Interna dentro de las organizaciones sea amplia y puede incluir temas de gobierno corporativo, gestión de valoración de riesgos, y el cumplimiento de leyes y reglamentos.

Madariaga Gorocica, Juan (2004), en su libro “Manual Práctico de Auditoría”, define a la Auditoría Interna como una actividad independiente que tiene lugar dentro de la empresa y que está encaminada a la revisión de operaciones contables y de otra naturaleza, con la finalidad de prestar un servicio a la dirección. Es un control de dirección que tiene por objeto la medida y evaluación de la eficacia de otros controles. La Auditoría Interna surge con posterioridad a la auditoría externa por la necesidad de mantener un control permanente y más eficaz dentro de la empresa. (p.25)

Comentario:

Según el autor Juan Madariaga (2004) considera que la Auditoría Interna es una actividad independiente que brinda un servicio a la Alta Dirección, teniendo como alcance las operaciones contables y los procesos internos de las empresas, cuyo propósito es asegurar que los controles establecidos por la Alta Dirección sean eficientes y eficaces, esta labor de control se realiza de manera continua y

permanente; asimismo, la Auditoría Interna surge por la necesidad del crecimiento de las empresas donde se hace imposible el control directo de la Alta Dirección.

Nudman y Puyol (2008) en su obra titulada Manual de Auditoría Operativa, señala que la auditoría operativa es examen crítico, sistemático e imparcial de la administración de una entidad, para determinar la eficacia con que logra los objetivos pre-establecidos y la eficiencia y economía con que se utiliza y obtiene los recursos, con el objeto de sugerir las recomendaciones que mejoraran la gestión en el futuro. (p.12)

Comentario:

Según Nudman y Puyol (2008) indica que la Auditoría Interna es una evaluación realizada por un profesional imparcial, ajeno al área auditada y que se desarrolla mediante procedimientos de control, a fin de determinar el cumplimiento de los objetivos establecidos por la entidad, y como resultado de esta labor se emite un informe con recomendaciones que agregan valor y mejoras a las operaciones, contribuyendo a los objetivos y metas de la entidad.

Pardo Vega, Julio (2009), en su libro titulado Fundamentos de la Auditoría Administrativa, señala que la auditoría administrativa es el examen y evaluación del proceso administrativo de una empresa, con el objeto de emitir recomendaciones constructivas que, optimicen la obtención de la información y efectividad en las operaciones y contribuyan al cumplimiento de sus metas y objetivos.(p.9)

Comentario:

Según Pardo Julio, (2009) nos expresa el autor que este examen es efectuado por profesionales con un profundo entendimiento de la cultura, los sistemas y procesos de los negocios, la actividad de

la auditoría asegura que los controles internos establecidos sean adecuados para mitigar los riesgos, los procesos de gobierno sean eficaces y eficientes, y las metas y objetivos de la organización se cumplan.

2.3.2 Y: GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Morales, Juan Carlos (2017), en su libro titulado “Dirección Eficaz de Tecnología de la Información” define como un Sistema de Gestión de Seguridad de la Información (SGSI) es un enfoque de sistemas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar de manera continua la seguridad de la información de una organización. Consta de políticas, procedimientos, guías, recursos y actividades asociadas, administradas por una organización, para proteger la información mediante la aplicación de un proceso de gestión de riesgos. El sistema de gestión de seguridad de la información debe estar integrado con los procesos de la organización y con las estructuras de gobierno y gestión. (p. 53)

Comentario:

Según Juan Carlos Morales (2017) se entiende por seguridad de la información a todas aquellas medidas preventivas que permitan resguardar y proteger la información de las organizaciones, y para por contar con una adecuada gestión de la información deben respaldarse mediante políticas y procedimientos administrados por la organización. Cabe señalar, que la gestión de la información debe encontrarse integrada a los procesos claves y a la estructuras de gobierno y gestión de la organización.

Gutierrez Jaime y Juan Tena (2003) en su libro Protocolos Criptográficos y Seguridad en Redes definen a la Gestión de la Seguridad de la Información al conjunto de medidas de seguridad que tienen por objeto proteger la información procesada,

almacenada o transmitida, por sistemas de comunicaciones, sistemas de información u otros tipos de sistemas electrónicos, contra la perdida de confidencialidad, integridad o disponibilidad, ya sea accidental o intencionada, e impedir la pérdida de la integridad y de la disponibilidad de los propios sistemas. (p.12)

Comentario:

Según Gutierrez Jaime y Juan Tena (2003) consideran que la Gestión de la Seguridad de la Información tiene como objetivo principal es proteger la información que se almacena en los diferentes sistemas y dispositivos de las empresas, preservando los tres pilares de la seguridad de la información que son confidencialidad, integridad y disponibilidad, considerando que en estos tiempos la información es un bien muy importante para las empresas y se considera prioridad en su manejo y control solo a personal autorizado.

Baca Urbina Gabriel (2016) en su libro Introducción a la Seguridad Informática señala que la seguridad informática es la disciplina que con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando riesgos tanto físicos como lógicos, a los que está expuestos. Esta definición se puede complementar señalando que en caso de que una amenaza a la seguridad se haga efectiva, debe procurar recuperar la información dañada o robada. (p.12)

Comentario:

Según Gabriel Urbina (2016) señala que para mantener un sistema de gestión de la información seguro y confiable en las empresas se debe contar con una base de políticas, normas internas y externas formalmente establecidas, la cual sirvan como respuesta inmediata

ante cualquier tipo de amenaza que atente a la seguridad de la información, y que estas acciones logren mitigar el impacto en las operaciones de la empresa por perdida de información.

Gomez Vieite, Alvaro (2014) en su libro Enciclopedia de la Seguridad Informática define a la Gestión de la Seguridad de la Información como aquella parte del sistema general de gestión que comprende la política, la estructura organizativa, los recursos necesarios, los procedimientos y los procesos necesarios para implementar la gestión de la seguridad de la información en una organización. Para gestionar la seguridad de la información es preciso contemplar toda una serie de tareas y de procedimientos que permitan garantizar los niveles de seguridad exigibles en una organización, teniendo en cuenta que los riesgos no se pueden eliminar totalmente, pero sí se pueden gestionar. (p.22)

Comentario:

Según Alvaro Gomez (2014) comenta que la Gestión de Seguridad de la Información corresponde a un proceso sistemático que abarca a toda la organización, a fin de que sean gestionadas mediante políticas y procedimientos que permitan planificar e implementar controles de seguridad basados en una evaluación de los riesgos empresariales, garantizando niveles de seguridad aceptables ante incidentes causados voluntaria o involuntariamente en la empresa o causados por factores externos (desastres naturales).

Wikipedia (2008) en el artículo titulado “Seguridad de la Información” define a la seguridad informática es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma. Para el hombre como individuo, la seguridad de la información tiene un efecto

significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo. Recuperado de: https://es.wikipedia.org/wiki/Seguridad_de_la_información

Comentario:

Según Wikipedia (2008) sostiene que la Gestión de la Seguridad de la Información proporciona un nivel de aseguramiento y protección de los sistemas y los activos de información en las empresas, con el propósito de implementar los tres pilares básicos de la seguridad de la información (confidencialidad, integridad y disponibilidad) que se complementan con las políticas y planes de acción establecidas en las organizaciones; asimismo, menciona el impacto significativo que conlleva el riesgo reputacional o imagen empresarial por fuga de información.

2.3.3 GLOSARIO DE TÉRMINOS

LA AUDITORIA INTERNA Y LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Independencia

Los auditores internos son independientes cuando pueden realizar su trabajo libre y objetivamente. La independencia permite a los auditores internos emitir juicios imparciales y equilibrados, lo cual es esencial para realizar adecuadamente los trabajos.

Objetividad

Los auditores internos exhiben el más alto nivel de objetividad profesional al reunir, evaluar y comunicar información sobre la actividad o proceso a ser examinado. Los auditores internos hacen una evaluación equilibrada de todas las circunstancias relevantes y forman sus juicios sin dejarse influir indebidamente por sus propios intereses o por otras personas.

Valor Agregado

Valor agregado o valor añadido es una característica o servicio extra que se le da a un producto o servicio, con el fin de darle un mayor valor comercial, generalmente se trata de una característica o servicio poco común, o poco usado por los competidores, y que le da al negocio o empresa, cierta diferenciación.

Control Interno

Es el conjunto de acciones, actividades, planes, políticas, normas, registros, procedimientos y métodos, incluido el entorno y actitudes que desarrollan autoridades y su personal a cargo, con el objetivo de prevenir posibles riesgos que afectan a una entidad pública o privada. Su estructura se basa en cinco componentes funcionales: Ambiente de control, Evaluación de riesgos, Actividades de control gerencial, Información y comunicación y Supervisión.

Acciones de Control

Son procedimientos que ayudan a asegurar que las políticas de la dirección se lleven a cabo, y deben estar relacionadas con los riesgos que ha determinado y asume la dirección. Las actividades de control se ejecutan en todos los niveles de la organización y en cada una de las etapas de la gestión, partiendo de la elaboración de un mapa de riesgos, conociendo los riesgos se disponen los controles destinados a evitarlos o minimizarlos.

Evaluación de Riesgos

Es uno de los pasos que se utiliza en un proceso de gestión de riesgos. El riesgo R se evalúa mediante la medición de los dos parámetros que lo determinan, la magnitud de la pérdida o daño posible L, y la probabilidad p que dicha pérdida o daño llegue a ocurrir.

Eficiencia y eficacia

La eficiencia se refiere a hacer las cosas bien, es obtener el mejor o máximo rendimiento utilizando un mínimo de recursos. La eficacia, por otra parte, es hacer las cosas de la manera correcta y de esta manera alcanzar el resultado deseado.

Aceptación de Riesgo

Es la decisión de recibir, reconocer, tolerar o admitir un riesgo. Esta decisión se toma una vez que se han estudiado los diferentes escenarios posibles para una misma amenaza y se han aplicado todos los procedimientos posibles para contrarrestar sus efectos y probabilidad de que ocurra.

Segregación de Funciones

Es un método que usan las organizaciones para separar las responsabilidades de las diversas actividades que intervienen en la

elaboración de los estados financieros, incluyendo la autorización y registro de transacciones así como mantener la custodia de activos.

Prevención de Acciones Fraudulentas

Es el análisis para evitar crear, acceder, eliminar, modificar, alterar, divulgar o usar activos de información de manera inapropiada con fines indebidos o para beneficio personal.

Políticas y Nomas de Seguridad de la Información

Son una serie de instrucciones documentadas que indican la forma en que se llevan a cabo determinados procesos dentro de una organización, también describen cómo se debe tratar un determinado problema o situación. Este documento está dirigido principalmente al personal interno de la organización, aunque hay casos en que también personas externas quedan sujetas al alcance de las políticas.

Accesos críticos y sensibles

En la seguridad de la información accesos críticos corresponde a actividades que son indispensables para la operación de la empresa y sensible son aquellos accesos que deben de ser asignadas u otorgadas a determinadas personas autorizadas.

Privilegios de Usuarios

Comprende los permisos para realizar una acción, asignable a un usuario o un rol en un sistema productivo de una empresa.

Análisis de los hechos

Es el estudio que realizan los auditores internos para cerciorarse de todos los aspectos que permitan definir si un hecho o una transacción están en forma correcta o es motivo de un hallazgo u observación de auditoría.

Comprobación

La comprobación es una técnica de auditoría que se aplica como parte de los procedimientos contenidos en los programas de auditoría y que permite cerciorarse sobre un evento, una transacción, sus formalidades, su valoración, su registro, presentación correcta o incorrecta.

Evaluación

La evaluación en Auditoría Interna es el examen que se realiza a la institución en general o en particular a una dependencia o un proceso o procedimiento.

Planeamiento de la auditoría

El planeamiento es una fase de la auditoría en el cual se provisionan todos los elementos para llevar a cabo la auditoría. Es la fase que marca la pauta de la auditoría y en base al cual se ejecuta e informa la auditoría.

Políticas

Las políticas son guías para orientar la acción; son lineamientos generales a observar en la toma de decisiones, sobre algún problema que se repite una y otra vez dentro de una organización.

Procedimientos de Auditoría Interna

Los procedimientos de Auditoría Interna representan actos que se realizan durante el curso de un examen mediante la aplicación de técnicas apropiadas. Un método o plan de acción usado para determinar la validez de los principios y normas.

Técnicas de la Auditoría Interna

Son los recursos particulares de investigación, utilizados por el auditor para obtener los datos necesarios para corroborar la información que ha obtenido o le han suministrado. Son los

métodos prácticos de investigación y prueba que el Contador público utiliza para lograr la información y comprobación necesaria para poder emitir su opinión profesional.

Acción Correctiva

Las acciones tomadas por la Administración basadas en la retroalimentación de los resultados de una auditoría o acción de control.

Apetito de Riesgo

Es la cantidad de riesgo a nivel global, que la administración está dispuesto a aceptar en su búsqueda de valor. Este puede ser establecido en relación a la organización como un todo, para diferentes grupos de riesgos o en un nivel de riesgo individual.

Control de riesgos

La parte del Proceso de Gestión del Riesgo que involucra la implementación de políticas, estándares, procedimientos y cambios físicos para eliminar o minimizar riesgos advertidos.

Criticidad:

Característica que se fundamenta entre otras variables, en el nivel del riesgo y en su importancia estratégica.

Impacto:

Consecuencia que puede ocasionar a la organización la materialización del riesgo. Puede haber más de una consecuencia de un mismo evento. Las consecuencias pueden estar en el rango de positivas a negativas. Las consecuencias se pueden expresar cualitativa o cuantitativamente. Las consecuencias se determinan en relación con el logro de objetivos.

Incertidumbre:

Una condición donde el resultado sólo puede ser estimado y no medido.

Matriz de Riesgos Estratégica:
Una herramienta usada para dar sistematizar el análisis de los procesos, sus riesgos, la severidad de los mismos, los controles asociados y la exposición al riesgo que presenta cada uno.

Monitorear:
Verificar, supervisar, observar críticamente o medir el progreso de una actividad, acción o sistema en forma regular para identificar cambios respecto del nivel de desempeño requerido o esperado.

Probabilidad:
La posibilidad de ocurrencia de un resultado o riesgo específico. La probabilidad se puede expresar en términos cuantitativos, mediante escalas que identifiquen niveles desde muy improbables hasta casi certeza.

Proceso:
Conjunto de actividades íntimamente relacionadas que existen para generar un bien o un servicio, que cuentan con un ingreso de recursos, una transformación de éstos y una salida de servicios o productos, que tienen un cliente interno o externo a la organización.

Servicios de Aseguramiento:
Un examen objetivo de evidencias con el propósito de proveer una evaluación independiente de los procesos de gestión de riesgos, control y gobierno de una organización.

ABAP/4
Lenguaje de Programación de SAP. Consultor ABAP es el especialista que programa en el lenguaje ABAP.

Ambiente de Desarrollo

Lugar de la infraestructura tecnológica en donde los consultores realizan la parametrización del sistema Lenguaje de Programación de SAP.

Transacción SAP

Operaciones que se realizan en el sistema SAP, para llevar el control y mantenimiento de la producción en la empresa

ERP (Enterprise Resource Planning)

Son sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con muchas operaciones de la empresa.

Key User

Es el administrador asignado por el área de administración que se encarga de asignar y regular los roles de usuarios, con la finalidad de tener controlado las acciones y movimiento de los usuarios.

Conflicto SAP

Se genera cuando un usuario ejecuta transacciones que se encuentran dentro de su rol de usuario, pero que por políticas de la empresa no debe de ejecutarlas

Rol de Usuario

Es un conjunto de transacciones que se encuentran clasificadas para cada área de la empresa y que son asignadas a cada usuario por parte del key user.

Segregación de Funciones (Separation of Duties - SOD)

Es el concepto de tener más de una persona para completar un proceso sensible como método de control interno destinado a prevenir el fraude o error. El análisis de Segregación de Funciones

tiene por objetivo controlar que un Colaborador no pueda llevar a cabo todas las fases de un proceso sensible, o en su defecto evidenciar la existencia del riesgo.

Validador de Accesos

Usuario de negocio experto y conocedor del modelo autorizaciones SAP quien tiene como responsabilidad de: Analizar y canalizar los requerimientos de accesos a los autorizadores detallando las actividades y las restricciones.

Autorizador por Jerarquía

Jefatura o Gerencia inmediata al Colaborador (de acuerdo a la estructura organizacional de la empresa) que tiene a su cargo un Usuario SAP.

Autorizador por Proceso

Jefatura o Gerencia responsable de un proceso de negocio dentro de la organización de la empresa.

Autorizador por Sociedad

Gerencia designada en una empresa, quien tiene la responsabilidad de aprobar o rechazar la aceptación de riesgos presentada por el Autorizador por Jerarquía concediendo accesos que generan conflicto de segregación de funciones.

CAPÍTULO III
HIPOTESIS Y VARIABLES

FORMULACIÓN DE HIPÓTESIS

3.1. HIPÓTESIS PRINCIPAL

La Auditoría Interna incide favorablemente en la optimización de la Gestión de Seguridad de la información de los usuarios del sistema SAP en empresas de servicios logísticos de la Provincia Constitucional del Callao, año 2016-2017, contribuyendo en la identificación de los riesgos en las empresas.

3.2 HIPÓTESIS SECUNDARIAS

a. El grado de independencia y objetividad incide adecuadamente en el plan de seguridad de la información de los usuarios del sistema SAP, con participación del auditor de manera imparcial.

b. El nivel de aporte de valor agregado incide satisfactoriamente en el logro de los objetivos y metas de la Gestión de Seguridad de la información de los usuarios del sistema SAP, cooperando en la mejora continua de las empresas.

c. El nivel del sistema de control interno incide adecuadamente en el grado de aceptación del riesgo de la organización en la Gestión de Seguridad de la información de los usuarios del sistema SAP, evaluando los riesgos de las empresas.

d. Las acciones de control inciden en la efectividad de las operaciones de la Gestión de Seguridad de la información de los usuarios del sistema SAP, impulsando el cumplimiento de las normas y procedimientos.

e. El seguimiento de las recomendaciones incide satisfactoriamente en el grado de eficiencia y eficacia de la Gestión de Seguridad de la información de los usuarios del sistema SAP, potenciando los controles en las empresas.

f. Los informes de auditoría incide razonablemente en el fortalecimiento de las políticas y normas de la seguridad de la información de los usuarios del sistema SAP, mejorando los niveles de gestión en las empresas.

3.3 OPERACIONALIZACIÓN DE VARIABLES

3.3.1 VARIABLE INDEPENDIENTE

X: AUDITORIA INTERNA

Definición Conceptual	Instituto de Auditores Internos (2013), señala que la Auditoría Interna, es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización.	
Definición Operativa	**Indicadores**	**Índices**
	X1. Grado de independencia y objetividad.	1.1 Libertad de condicionamientos. 1.2 Responsabilidad de forma imparcial. 1.3 Actitud mental independiente. 1.4 Nivel del juicio profesional.
	X2. Nivel de aporte de valor agregado a la empresa.	2.1 Toma de decisiones estratégicas. 2.2 Indicadores de Productividad. 2.3 Nivel de mejora continúa. 2.4 Rentabilidad de la empresa.
	X3. Evaluar nivel de Control Interno.	3.1 Ambiente de Control. 3.2 Autoevaluaciones. 3.3 Nivel de grado de madurez. 3.4 Porcentaje de prevención y monitoreo.
	X4. Acciones de control.	4.1 Nivel de desviaciones o irregularidades. 4.2 Valor de mitigación de riesgos. 4.3 Políticas y normas. 4.4 Cumplimiento normativo.
	X5. Seguimiento de recomendaciones.	5.1 Implementación de mejoras. 5.2 Nivel de Superación de Observaciones. 5.3 Ejecución de cambios en los procesos. 5.4 Indicadores de Gestión.
	X6. Informes de Auditoría Interna	6.1 Comités de Auditoría Interna. 6.2 Porcentaje de observaciones reiterativas. 6.3 Buenas prácticas y normas. 6.4 Nivel de satisfacción del auditado.
Escala Valorativa		Nominal

3.3.2 VARIABLE DEPENDIENTE

Y: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

<table>
<tr><td>Definición Conceptual</td><td colspan="2">Morales, J (2017) define como políticas, procedimientos, guías, recursos y actividades asociadas, administradas por una organización, para proteger la información mediante la aplicación de un proceso de gestión de riesgos.</td></tr>
<tr><td rowspan="7">Definición Operativa</td><td>Indicadores</td><td>Índices</td></tr>
<tr><td>Y1. Plan de Seguridad.</td><td>1.1 Nivel de continuidad de los negocios.
1.2 Políticas y procedimientos aprobados
1.3 Identificación del impacto en los negocios.
1.4 Indicador de funciones críticas.</td></tr>
<tr><td>Y2. Logro de Objetivos y Metas.</td><td>2.1 Planeamiento Estratégico.
2.2 Indicador clave de rendimiento (KPI´s).
2.3 Misión y Visión.
2.4 Identificación de los principales Macro-Procesos.</td></tr>
<tr><td>Y3. Evaluar el grado de aceptación del riesgo de la organización.</td><td>3.1 Mapeo de los riesgos en la empresa.
3.2 Nivel de Riesgo Inherente.
3.3 Medición del Apetito del Riesgo.
3.4 Evaluación de Riesgos por Sistemas.</td></tr>
<tr><td>Y4. Efectividad de operaciones.</td><td>4.1 Índice de efectividad.
4.2 Niveles de riegos identificados y valorados.
4.3 Control de Operaciones
4.4 Verificación de procesos</td></tr>
<tr><td>Y5. Grado de eficiencia y eficacia.</td><td>5.1 Meta y Objetivos
5.2 Planes de seguimiento.
5.3 Costo-Beneficio
5.4 Grado de Productividad</td></tr>
<tr><td>Y6. Fortalecimiento de las políticas y normas de la seguridad de la información.</td><td>6.1 Leyes y normas vigentes
6.1 Vulnerabilidad de la información.
6.2 Incidentes de seguridad
6.3 Concientización de los usuarios.
6.4 Identificación de información sensible.</td></tr>
<tr><td>Escala Valorativa</td><td></td><td>Nominal</td></tr>
</table>

CAPITULO IV
METODOLOGÍA

4.1 Diseño metodológico

4.1.1 Tipo de investigación

Por el tipo de investigación el estudio reúne las condiciones necesarias para ser denominada como una investigación Aplicada. La misma que busca la relacionar los conocimientos de la Auditoría Interna y su incidencia en la optimización de la gestión de seguridad de la información de los usuarios del sistema SAP en las empresas de servicios logísticos en la Provincia Constitucional del Callao. Conforme a los propósitos del estudio la investigación se centra en la parte descriptiva – explicativa.

4.1.2 Nivel de investigación

En la presente investigación utilizamos el método descriptivo, y explicativa y otros que conforman su desarrollo de investigación seguirán utilizando indistintamente.

4.2 Población y muestra

4.2.1 Población

La población investigada estuvo conformada por 18 Auditores Internos y 83 funcionarios de las Empresas de Servicios de Logísticos en la Provincia Constitucional del Callao del año 2016-2017.

4.2.2 Muestra

Para determinar el tamaño óptimo de muestra se utilizó la fórmula del muestreo aleatorio simple para estimar proporciones cuya fórmula se describe a continuación:

$$n = \frac{Z^2\, pq\, N}{E^2\,(N-1) + Z^2\,(p*q)}$$

Dónde:

- Z: Valor de la abscisa de la curva normal para una probabilidad del 95% de confianza.
- p: Proporción de gerentes y auditores que manifestaron obtener beneficios en el control interno al evaluar la gestión de la empresa. (Se asume P = 0.5)
- q: Proporción de Gerentes, contadores y auditores que manifestaron no obtener beneficios en el control interno al evaluar la gestión empresarial (Se asume Q = 0.5)
- E: Margen de error 5%
- N: Población
- n: Tamaño óptimo de muestra.

Entonces, con un nivel de confianza de 95% y margen de error del 5% la muestra óptima es:

$$n = \frac{(1.96)^2 (0.5) (0.5) (101)}{(0.05)^2 (101-1) + (1.96)2 (0.5) (0.5)}$$

n = 80 entre Gerentes y Auditores Internos.

Calculo del Factor de Distribución Muestra (FDM)

$$FDM = \frac{n}{N} = \frac{80}{101} = 0.7921$$

N°	Empresa	Población Especializada Auditores y Funcionarios	FDM
1	Ransa Comercial	08	6
2	Agencias Ransa	06	5
3	Almacenera del Perú	21	17
4	Procesadora Torre Blanca	04	3
5	Servicios Logísticos Automotrices	06	5
6	Depósitos Especiales	05	4
7	Trabajos Marítimos	10	8
8	Ransa Operador Logístico Bolivia	08	6
9	Neptunia SA	20	16
10	Sagitario Operador Logístico	13	10
	Total	**101**	**80**

Fuente-Propia

4.3 Técnicas de recolección de datos

4.3.1 Técnicas

La principal técnica que se utilizó en la investigación es la encuesta la misma que se aplicó a Gerentes y Auditores Internos de empresas de servicios logísticos.

4.3.2 Procedimientos de comprobación de la validez y confiabilidad de los instrumentos

Para procesar la información se utilizó los instrumentos siguientes: Un cuestionario de preguntas cerradas, que permitió establecer la situación actual y alternativas de solución a la problemática que se establece en la presente investigación.

4.4 Técnicas para el procesamiento de la información

Se tabuló la información a partir de los datos obtenidos haciendo uso del programa computacional SPSS (Statiscal Package for Social Sciences) versión 22, del modelo de correlación de Pearson y nivel de confianza del 95%.

4.5 Aspectos éticos

El presente trabajo tiene como objetivo principal demostrar el aporte de la Auditoría Interna en la optimización de la Gestión de Seguridad de la Información de los usuarios del Sistema SAP de las Empresas de Servicios Logísticos, considerando que en el Código de Ética de la Universidad San Martin de Porres aprobado en Abril 2008, establece que:

Artículo 6.- Búsqueda de la verdad

6.1.- Se debe buscar la verdad como valor implícito a la función de la Universidad, es una pauta de conducta que debe guiar los actos de todos sus integrantes, es su suprema aspiración: veritas liberabit vos. (La verdad nos hará libres).

Artículo 7.- Honestidad, integridad y cumplimiento de compromiso

7.3.- Honestidad intelectual
7.3.1 Los profesores y alumnos actúan con honestidad intelectual al respectar la autoría, diseños e ideas de las fuentes de información consultadas o utilizadas para la elaboración de trabajos de investigación, monografías, ayudas audiovisuales u otros. Es inaceptable el plagio, en todas sus manifestaciones y en todos los ámbitos de la Institución.

Asimismo, el Código de Ética Profesional del Contador Público aprobado por la Junta de Decanos de Colegios de Contadores Públicos del Perú en Junio 2007, establece que:

Artículo 5º. En el ejercicio profesional, el Contador Público Colegiado actuará con probidad y buena fe, manteniendo el honor, dignidad y capacidad profesional, observando las normas del Código de ética en todos sus actos.

CAPÍTULO V
RESULTADOS

5.1 INTERPRETACIÓN DE RESULTADOS

A continuación presentamos los resultados estadísticos a los que se han llegado luego de la aplicación de la encuesta a 80 colaboradores, conformados por auditores internos y funcionarios de empresas de servicios logísticos en la Provincia Constitucional del Callao. Debemos indicar que la información fue procesada en el software SPSS V22 y se obtuvo la siguiente información:

5.1.1 Auditoría Interna independiente y objetiva

Pregunta N°01 - ¿Está de acuerdo que el Auditor debe tener un grado independencia y objetividad para desarrollar su trabajo en las empresas?

TABLA N°01

Alternativas	Auditores y funcionarios	Porcentaje
De acuerdo	10	12,5
Totalmente de acuerdo	62	77,5
Ni de acuerdo ni en desacuerdo	6	7,5
En desacuerdo	1	1,3
Totalmente en desacuerdo	1	1,3
Total	80	100.0

Interpretación

La importancia de la labor del Auditor en toda empresa se ve reflejado en el informe y en las recomendaciones que pueda facilitar de manera objetiva. Por lo que la mayoría de Auditores y funcionarios de las empresas de Servicios Logísticos en la Provincia Constitucional del Callao, 77,5%, señaló estar totalmente de acuerdo que en el mejor de los casos el Auditor debe tener un grado de independencia y objetividad al realizar su trabajo, aunque otro 1,3% de estos funcionarios y auditores afirmaron estar totalmente en desacuerdo con la independencia y objetividad de los auditores.

Análisis

Según la información obtenida, el 77,5% de los encuestados respondieron que es importante que las labores de Auditoría Interna se realicen con un grado de independencia y objetividad en las empresas de servicios logísticos.

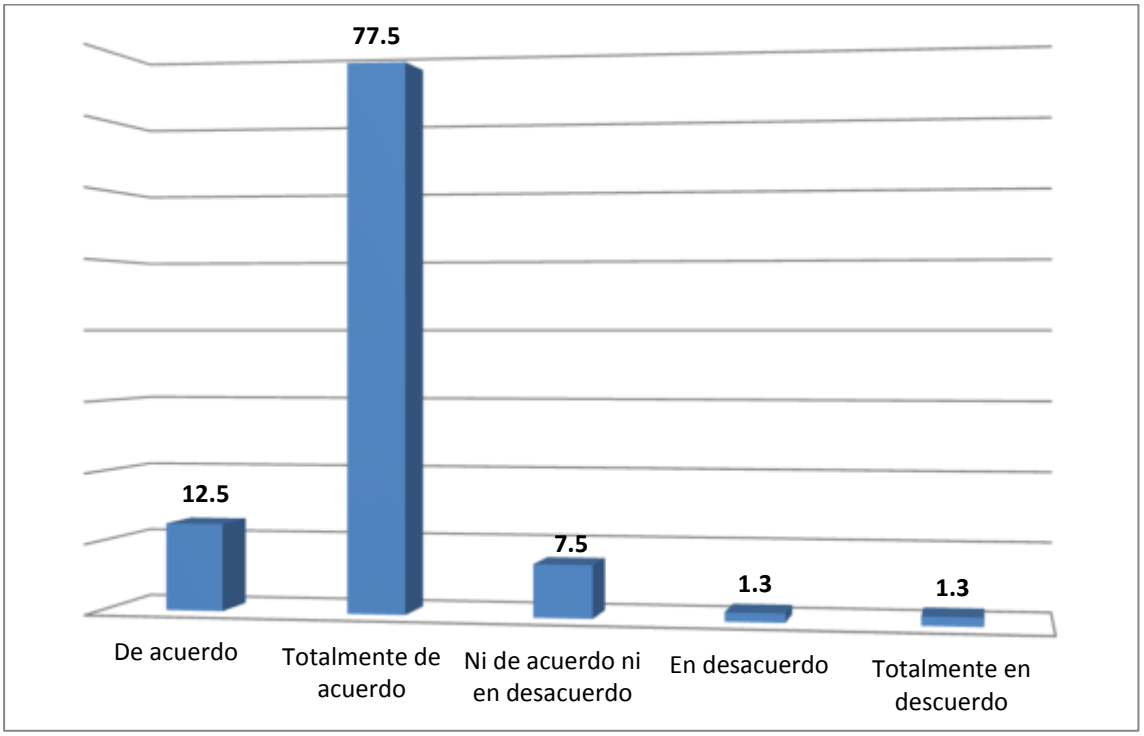

Figura 1. El Auditor debe tener un grado de independencia y objetividad

Fuente. Tabla N°01

5.1.2 Valor agregado de la Auditoría Interna en las Empresas

Pregunta N° 02 - ¿Diga usted, si el valor agregado del trabajo del auditor son las recomendaciones contenidas en la carta de control interno en las empresas?

TABLA N°02

Alternativas	Auditores y funcionarios	Porcentaje
De acuerdo	12	15,0
Totalmente de acuerdo	66	82,5
Ni de acuerdo ni en desacuerdo	1	1,3
En desacuerdo	1	1,3
Totalmente en descuerdo	0	0,0
Total	80	100.0

Interpretación

La mayoría de Auditores y funcionarios de las empresas de Servicios Logísticos en la Provincia Constitucional del Callao, 82,5%, afirmó estar totalmente de acuerdo que valor agregado del trabajo del auditor son las recomendaciones contenidas en la carta de control interno, Sin embargo, otro 1,3% de funcionarios y auditores sostuvieron estar en desacuerdo con lo señalado anteriormente, es decir, que valor agregado del trabajo del auditor no son precisamente las recomendaciones contenidas en la carta de control interno de la empresa.

Análisis

Según la información obtenida, el 82.5% de los encuestados respondieron que es importante el valor agregado que se plasman mediante las recomendaciones de Auditoría Interna en las empresas de servicios logísticos.

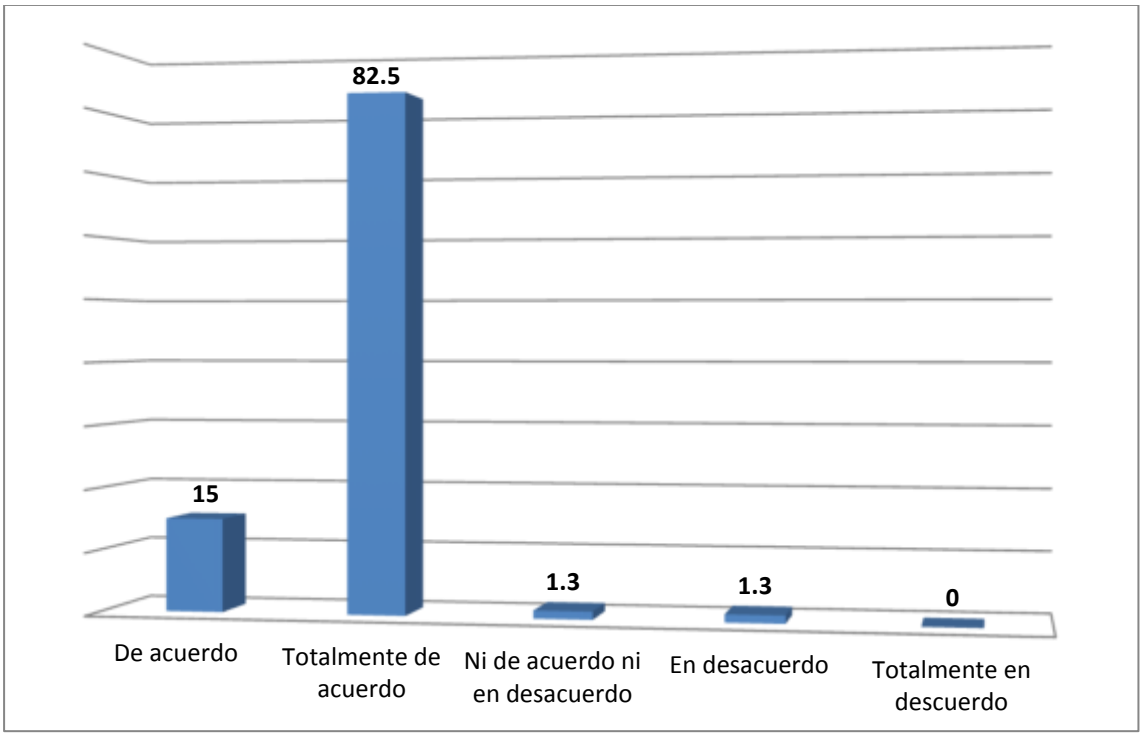

Figura 2. El valor agregado del trabajo del auditor son las recomendaciones contenidas en la carta de control interno en las empresas

Fuente. Tabla N° 02

5.1.3 El Auditor Interno y el nivel de control implementado en empresas

Pregunta N° 03 - ¿En su opinión, el Auditor debe evaluar el nivel de control interno implementado en las empresas?

TABLA N°03

Alternativas	Auditores y funcionarios	Porcentaje
De acuerdo	10	12,5
Totalmente de acuerdo	68	85,0
Ni de acuerdo ni en desacuerdo	1	1,3
En desacuerdo	1	1,3
Totalmente en desacuerdo	0	0,0
Total	80	100.0

Interpretación

La mayoría de Auditores y funcionarios de las empresas de Servicios Logísticos en la Provincia Constitucional del Callao, 85%, afirmó estar totalmente de acuerdo que el Auditor debe evaluar el nivel de control interno implementado en las empresas. Pero, otro porcentaje mínimo, 1,3% de funcionarios y auditores coincidieron estar en desacuerdo con que el Auditor debe evaluar el nivel de control interno implementado en las empresas.

Análisis

Según la información obtenida, el 85% de los encuestados respondieron que es importante que el Auditor deba evaluar el sistema de control interno de las empresas de servicios logísticos.

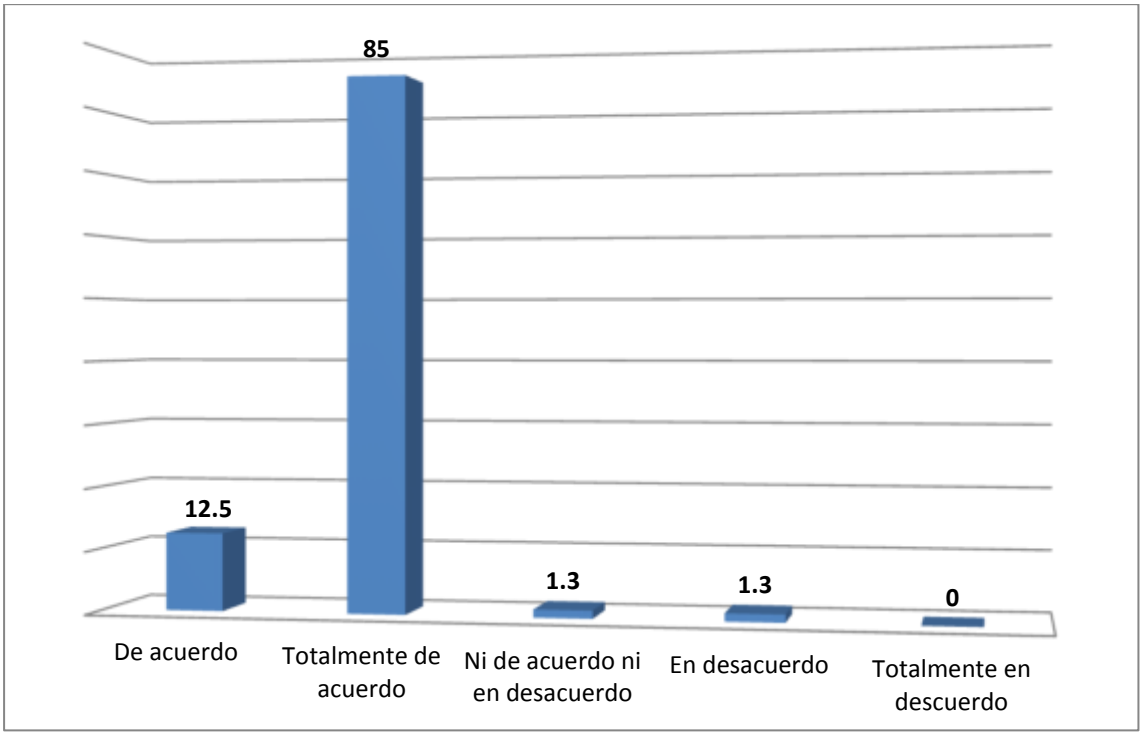

Figura 3. El Auditor debe evaluar el nivel de control interno implementado en las empresas

Fuente. Tabla N° 03

5.1.4 Las Acciones de Control en el Plan Anual de Control

Pregunta N° 04 - ¿Considera usted, que las acciones de control contenidas en el Plan Anual de Control se aplican oportunamente por Auditoría Interna?

TABLA N°04

Alternativas	Auditores y funcionarios	Porcentaje
De acuerdo	18	22,5
Totalmente de acuerdo	60	75,0
Ni de acuerdo ni en desacuerdo	1	1,3
En desacuerdo	1	1,3
Totalmente en descuerdo	0	0,0
Total	80	100.0

Interpretación

La mayoría de Auditores y funcionarios de las empresas de Servicios Logísticos en la Provincia Constitucional del Callao, 75%, sostuvo estar totalmente de acuerdo que las acciones de control contenidas en el Plan Anual de Control se aplican oportunamente por Auditoría Interna. Pero, un porcentaje mínimo, 1,3% de funcionarios y auditores afirmaron estar en desacuerdo con que las acciones de control contenidas en el Plan Anual de Control se aplican oportunamente por Auditoría Interna.

Análisis

De acuerdo a la información anterior, se aprecia que la mayoría de los consultados señalaron que es importante las acciones de control en el Plan de Anual de Control, lo que permitiría controlar o mitigar las operaciones que se hacen en las empresas de servicios logísticos.

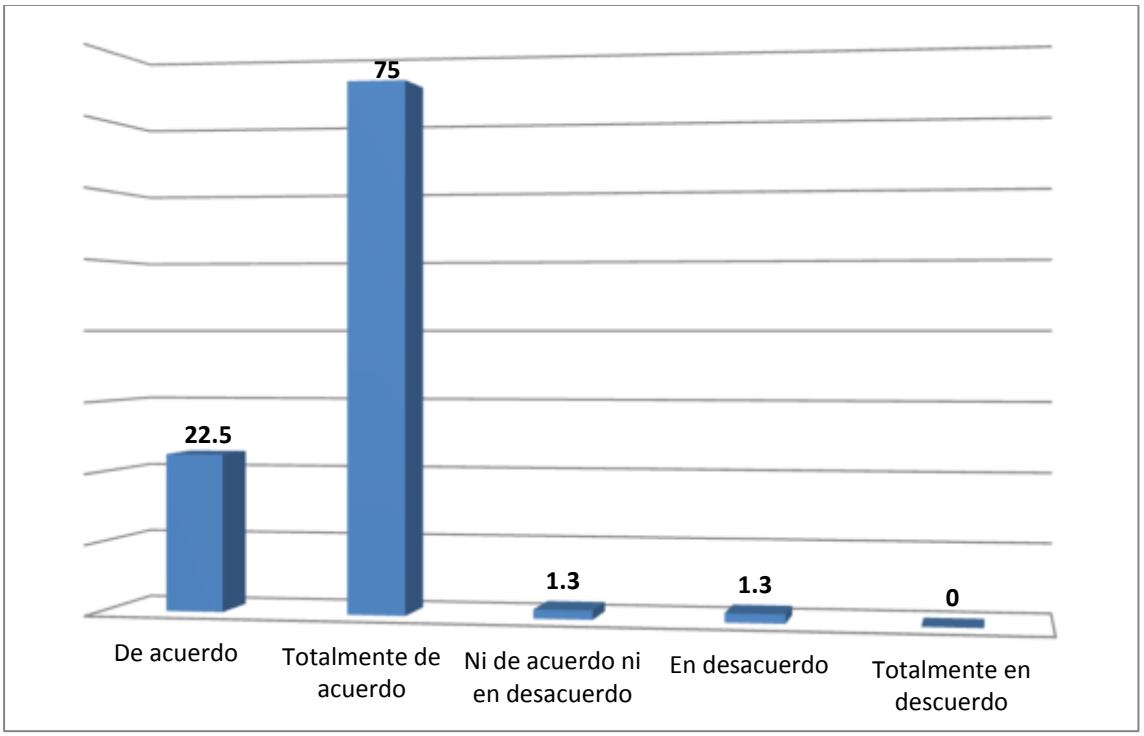

Figura 4. Las acciones de control contenidas en el Plan Anual de Control se aplican oportunamente por Auditoría Interna

Fuente. Tabla N°04

5.1.5 Recomendaciones de Auditoría como Herramienta de Gestión

Pregunta N° 05 - ¿Cree usted, que el seguimiento de recomendaciones contenidas en el Informe, constituye una herramienta de gestión para la mejora de las empresas?

TABLA N°05

Alternativas	Auditores y funcionarios	Porcentaje
De acuerdo	14	17,5
Totalmente de acuerdo	64	80,0
Ni de acuerdo ni en desacuerdo	1	1,3
En desacuerdo	1	1,3
Totalmente en descuerdo	0	0,0
Total	80	100.0

Interpretación

La mayoría de Auditores y funcionarios de las empresas de Servicios Logísticos en la Provincia Constitucional del Callao, 80%, sostuvo estar totalmente de acuerdo que el seguimiento de recomendaciones contenidas en el Informe, constituye una herramienta de gestión para la mejora de las empresas. Por otro lado, un porcentaje mínimo, 1,3% de funcionarios y auditores afirmaron estar en desacuerdo que el seguimiento de recomendaciones contenidas en el Informe, constituya una herramienta de gestión para la mejora de las empresas.

Análisis

De la información anterior, podemos indicar que mayoría de los consultados señalaron que las recomendaciones contenidas en los informes de Auditoría Interna si constituye principalmente una herramienta de gestión para la mejora continua de las empresas, pues permite identificar las debilidades de control interno en las áreas críticas de las empresas de servicios logísticos y tomar las medidas correctivas de manera oportuna.

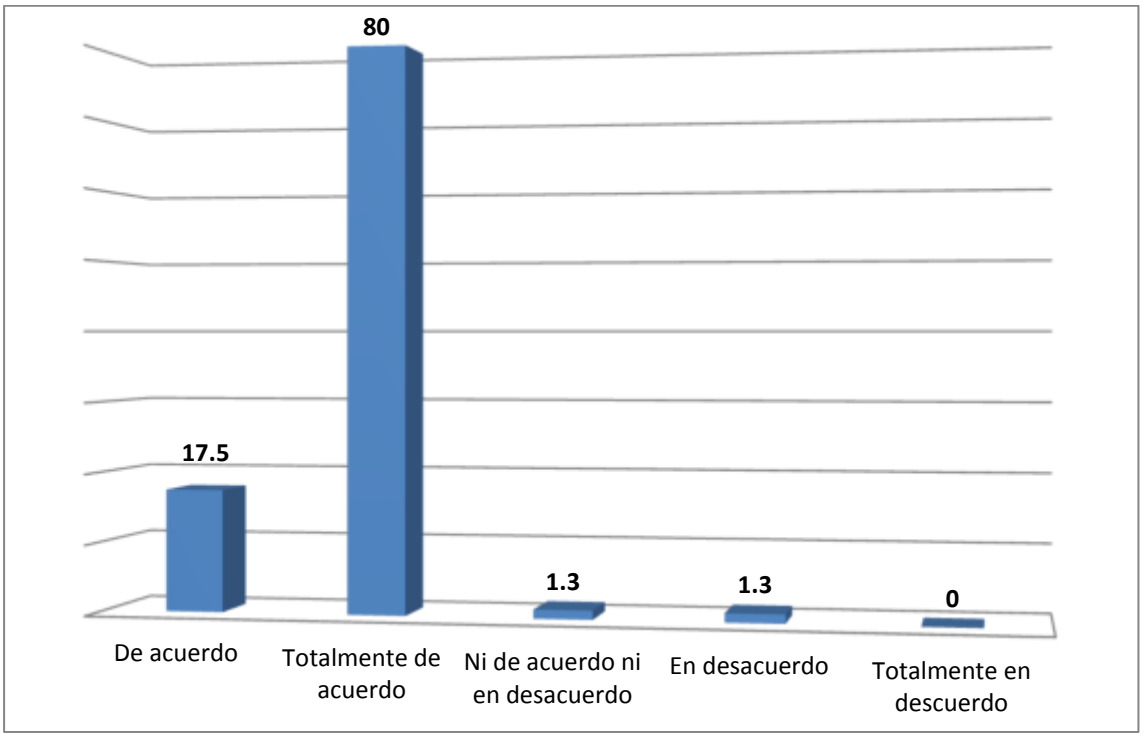

Figura 5. El seguimiento de recomendaciones contenidas en el Informe, constituye una herramienta de gestión para la mejora de las empresas

Fuente. Tabla N° 05

5.1.6 Los Informes de Auditoría contribuyen en la gestión de las empresas

Pregunta N° 06 - ¿Para usted, los Informes de Auditoría Interna contribuyen en el desarrollo de la gestión en las empresas?

TABLA N°06

Alternativas	Auditores y funcionarios	Porcentaje
De acuerdo	12	15,0
Totalmente de acuerdo	66	82,5
Ni de acuerdo ni en desacuerdo	1	1,3
En desacuerdo	1	1,3
Totalmente en descuerdo	0	0,0
Total	80	100.0

Interpretación

La mayoría de Auditores y funcionarios de las empresas de Servicios Logísticos en la Provincia Constitucional del Callao, 82,5%, está totalmente de acuerdo que los informes de Auditoría Interna contribuyen en el desarrollo de la gestión en las empresas. Sin embargo, un porcentaje mínimo, 1,3% de funcionarios y auditores afirmaron estar en desacuerdo que los informes de Auditoría Interna contribuyen en el desarrollo de la gestión en las empresas.

Análisis

De la información anterior, podemos indicar que mayoría de los consultados señalaron que los informes de Auditoría contribuyen en la gestión de las empresas de servicios logísticos; es decir, que con dicha información aporta observaciones y recomendaciones que contribuyen en alcanzar los objetivos de las empresas.

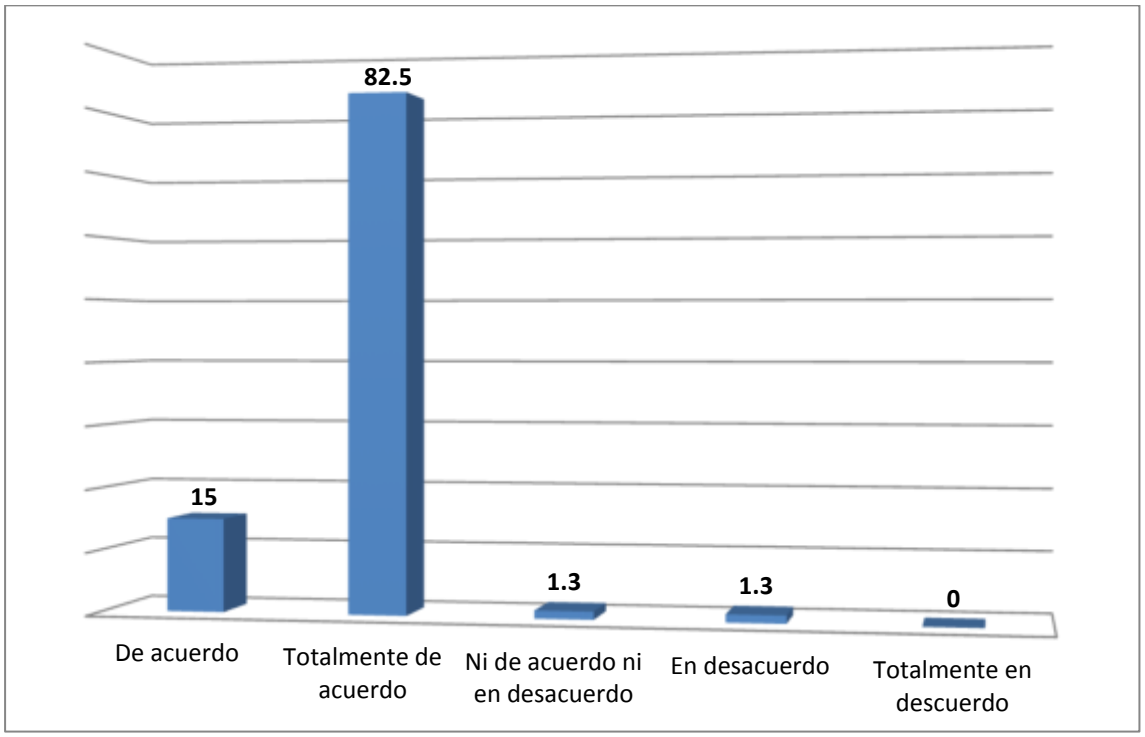

Figura 6. Los informes de Auditoría Interna contribuyen en el desarrollo de la gestión en las empresas

Fuente. Tabla N° 06

5.1.7 Auditoría Interna y las Empresas de Servicios Logísticos

Pregunta N° 07 - ¿Considera que la función de Auditoría Interna cumple un papel importante en las empresas de servicios logísticos?

TABLA N°07

Alternativas	Auditores y funcionarios	Porcentaje
De acuerdo	13	16,3
Totalmente de acuerdo	63	78,8
Ni de acuerdo ni en desacuerdo	2	2,5
En desacuerdo	1	1,3
Totalmente en descuerdo	0	0,0
Total	80	100.0

Interpretación

Una gran proporción de Auditores y funcionarios de las empresas de Servicios Logísticos en la Provincia Constitucional del Callao, 78,8%, está totalmente de acuerdo que la función de la Auditoría Interna cumple un papel importante en las empresas. Pero, un porcentaje mínimo, 1,3% de funcionarios y auditores afirmaron estar en desacuerdo con lo mencionado anteriormente.

Análisis

Podemos indicar que la mayoría de los consultados señalaron que la Auditoría Interna cumple un papel importante en las empresas de servicios logísticos; es decir, que al ser considerada como una actividad de evaluación independiente contribuyen en el fortalecimiento de los procesos, policías y procedimientos dentro de una organización.

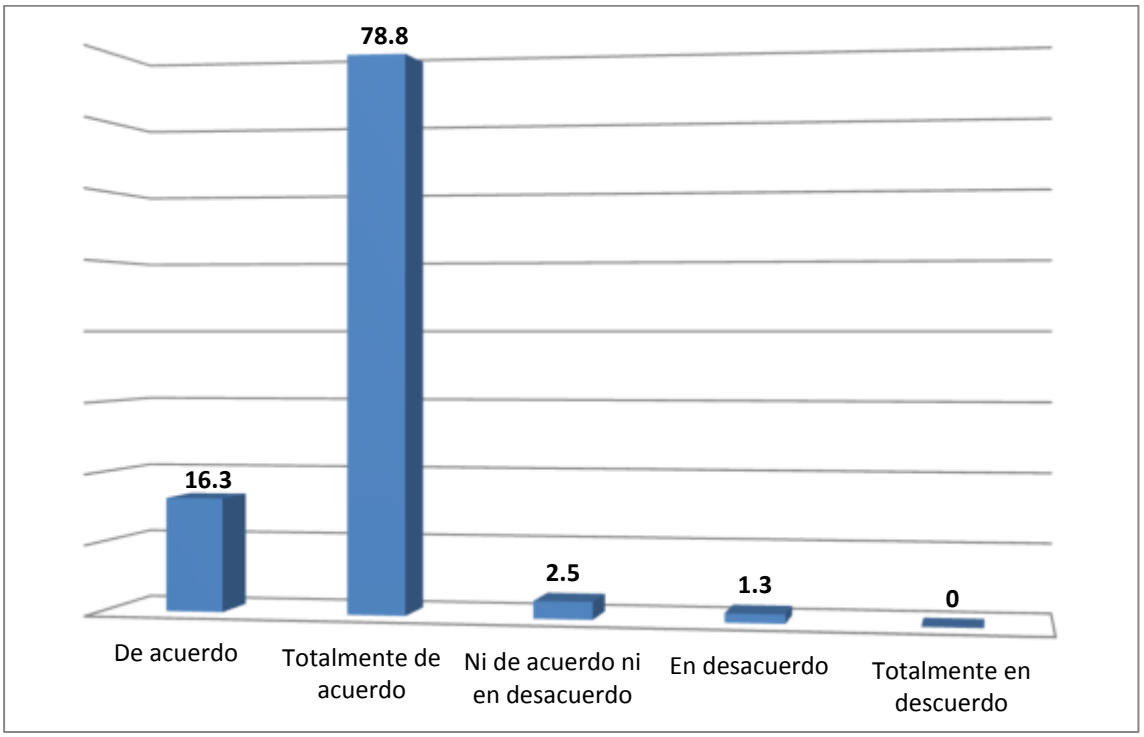

Figura 7. La función de Auditoría Interna cumple un papel importante en las empresas de servicios logísticos

Fuente. Tabla N°07

5.1.8 Los Planes de Seguridad y la prevención de los riesgos empresariales

Pregunta N° 08 - ¿Considera Ud., que los planes de seguridad aportan en la prevención de los riesgos en las empresas?

TABLA N°08

Alternativas	Auditores y funcionarios	Porcentaje
De acuerdo	25	31,3
Totalmente de acuerdo	52	65,0
Ni de acuerdo ni en desacuerdo	2	2,5
En desacuerdo	1	1,3
Totalmente en descuerdo	0	0,0
Total	80	100.0

Interpretación

Una buena proporción de Auditores y funcionarios de las empresas de Servicios Logísticos en la Provincia Constitucional del Callao, 65%, está totalmente de acuerdo que los planes de seguridad aportan en la prevención de los riesgos en las empresas de Servicios Logísticos. Pero, un porcentaje mínimo, 1,3% de funcionarios y auditores afirmaron estar en desacuerdo que los planes de seguridad aportan en la prevención de los riesgos.

Análisis

De la información anterior, podemos indicar que mayoría de los consultados señalaron que los Planes de Seguridad aportan en la prevención de los riesgos empresariales; es decir, que los Planes sirven como una herramienta de control, la cual permite establecer los riesgos asociados a las empresas establecer acciones que minimicen los riegos empresariales.

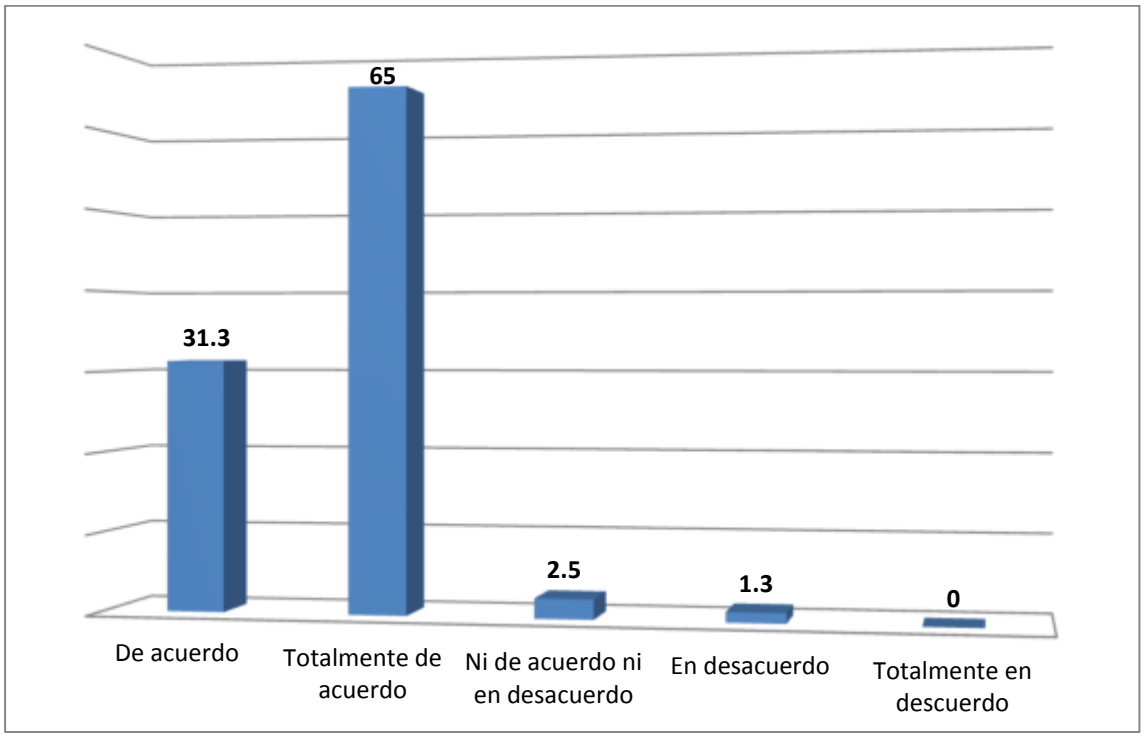

Figura 8. Los planes de seguridad aportan en la prevención de los riesgos en las empresas

Fuente. Tabla N° 08

5.1.9 Objetivos y metas en las empresas de servicios logísticos

Pregunta N° 09 - ¿Piensa Ud., que el logro de los objetivos y metas en las empresas de servicios logísticos, es adecuado?

TABLA N°09

Alternativas	Auditores y funcionarios	Porcentaje
De acuerdo	29	36,3
Totalmente de acuerdo	48	60,0
Ni de acuerdo ni en desacuerdo	1	1,3
En desacuerdo	2	2,5
Totalmente en descuerdo	0	0,0
Total	80	100.0

Interpretación

El 60% de Auditores y funcionarios de las empresas de Servicios Logísticos en la Provincia Constitucional del Callao, señaló que está totalmente de acuerdo que el logro de los objetivos y metas en las empresas de servicios logísticos, es el adecuado. Aunque, un porcentaje mínimo, 2,5% de funcionarios y auditores afirmaron estar en desacuerdo que el logro de los objetivos y metas en las empresas de servicios logísticos, sea el adecuado.

Análisis

De la información anterior, podemos indicar que mayoría de los encuestados señalaron que los objetivos y metas son adecuados; es decir, que favorecen en el desarrollo y gestión de las empresas de servicios logísticos.

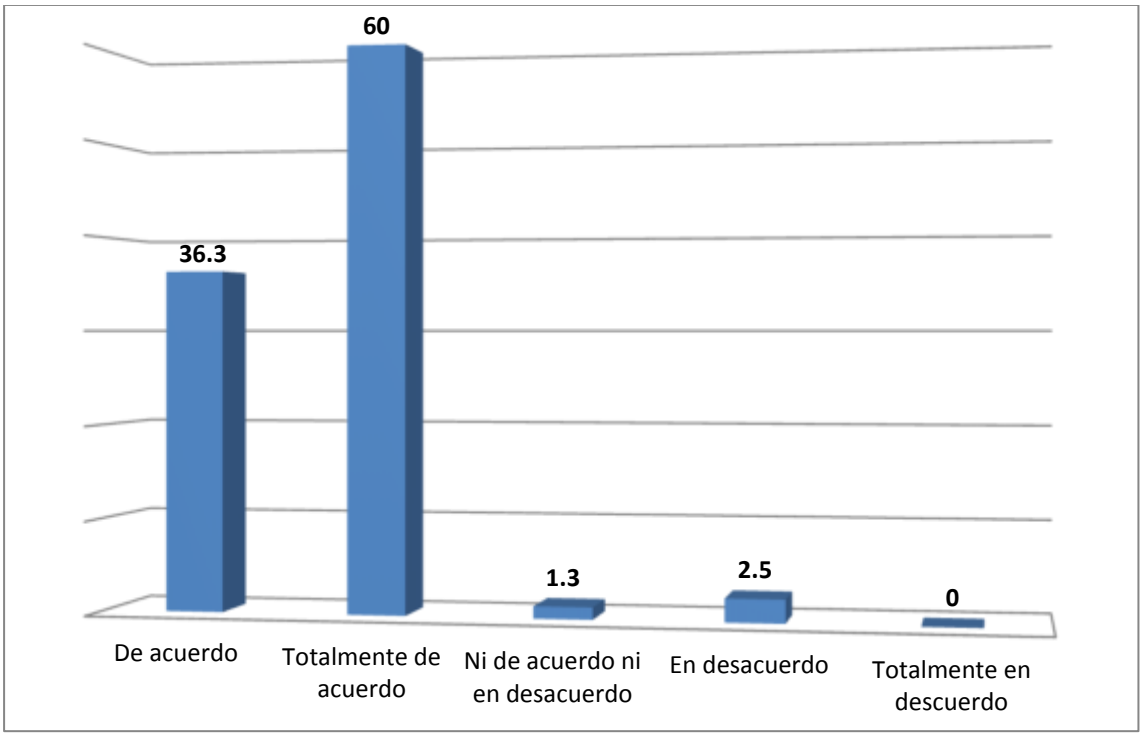

Figura 9. El logro de los objetivos y metas en las empresas de servicios logísticos, es adecuado

Fuente. Tabla N° 09

5.1.10 La Organización y la aceptación del riesgo

Pregunta N° 10 - ¿Para usted, ésta de acuerdo el grado de aceptación del riesgo de la organización es manejable o administrable?

Alternativas	Auditores y funcionarios	Porcentaje
De acuerdo	27	33,8
Totalmente de acuerdo	51	63,8
Ni de acuerdo ni en desacuerdo	0	0,0
En desacuerdo	2	2,5
Totalmente en descuerdo	0	0,0
Total	80	100.0

Interpretación

El 63.8% de Auditores y funcionarios de las empresas de Servicios Logísticos en la Provincia Constitucional del Callao, señaló estar totalmente de acuerdo que el grado de aceptación del riesgo de la organización es manejable. Aunque, un porcentaje mínimo, 2,5% de funcionarios y auditores afirmaron estar en desacuerdo que el grado de aceptación del riesgo de la organización es manejable.

Análisis

De la información anterior, podemos indicar que mayoría de los consultados señalaron que el grado de aceptación del riesgo es manejable o administrable; es decir, ayudan a las empresas a identificar, evaluar e implantar metodologías de gestión de riesgos y controles para tratar aquellos riesgos aceptados.

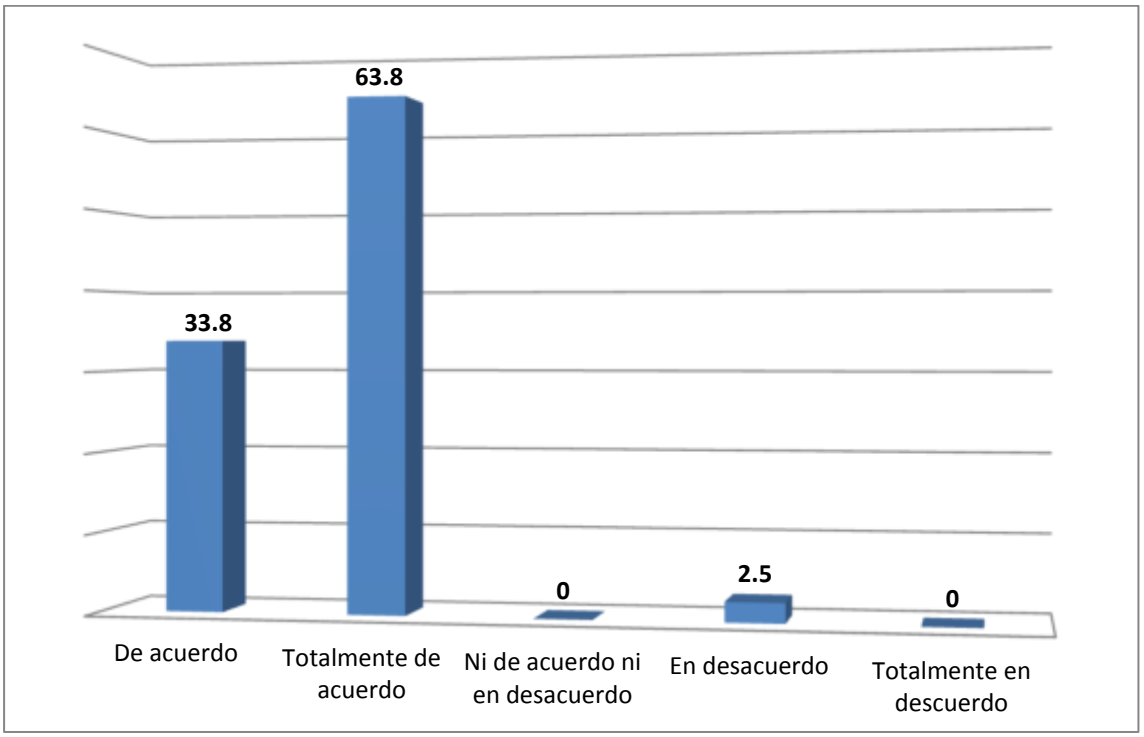

Figura 10. El grado de aceptación del riesgo de la organización es manejable

Fuente. Tabla N° 10

5.1.11 Efectividad de las operaciones reportadas de manera sustentada

Pregunta N° 11 - ¿Para usted, la efectividad de las operaciones son reportadas de manera sustentada en la empresa?

TABLA N°11

Alternativas	Auditores y funcionarios	Porcentaje
De acuerdo	29	36,3
Totalmente de acuerdo	48	60,0
Ni de acuerdo ni en desacuerdo	0	0,0
En desacuerdo	2	2,5
Totalmente en descuerdo	1	1,3
Total	80	100.0

Interpretación

El 60% de Auditores y funcionarios de las empresas de Servicios Logísticos en la Provincia Constitucional del Callao, señaló estar totalmente de acuerdo que la efectividad de las operaciones son reportadas de manera sustentada en la empresa. Pero, un porcentaje mínimo, 1,3% de funcionarios y auditores afirmaron estar en total desacuerdo que la efectividad de las operaciones son reportadas de manera sustentada a la empresa.

Análisis

De la información anterior, podemos indicar que mayoría de los consultados señalaron que la efectividad de las operaciones debe ser reportada de forma sustentada; es decir, que al contar con evidencia sustentatoria estas sirven de respaldo para medir la efectividad de las operaciones.

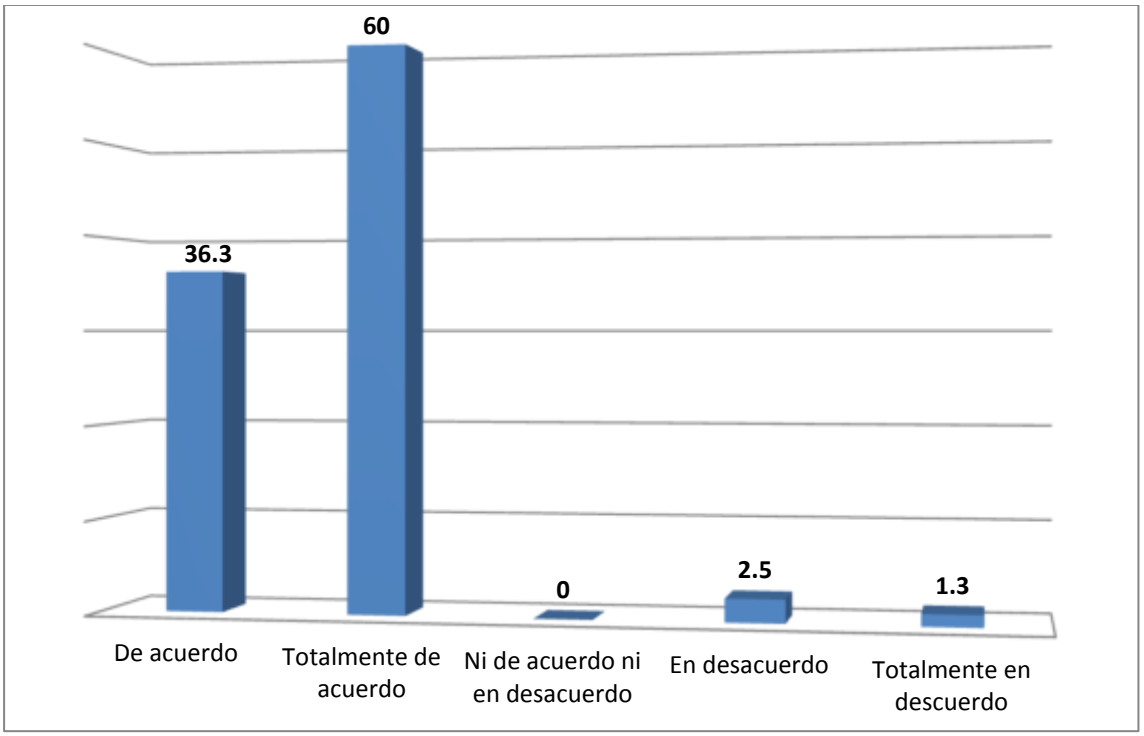

Figura 11. La efectividad de las operaciones son reportadas de manera sustentada en la empresa

Fuente. Tabla N° 11

5.1.12 El grado de eficiencia y eficacia con los resultados obtenidos

Pregunta N° 12 - ¿Considera usted, que el grado de eficiencia y eficacia tienen concordancia con los resultados obtenidos por las empresas?

TABLA N°12

Alternativas	Auditores y funcionarios	Porcentaje
De acuerdo	23	28,8
Totalmente de acuerdo	53	66,3
Ni de acuerdo ni en desacuerdo	1	1,3
En desacuerdo	2	2,5
Totalmente en descuerdo	1	1,3
Total	80	100.0

Interpretación

La mayoría de Auditores y funcionarios de las empresas de Servicios Logísticos en la Provincia Constitucional del Callao, 66,3%, afirmó estar totalmente de acuerdo que el grado de eficiencia y eficacia tienen concordancia con los resultados obtenidos por las empresas. Por otro lado, 1,3% de funcionarios y auditores manifestaron estar en total desacuerdo que el grado de eficiencia y eficacia tienen concordancia con los resultados obtenidos por las empresas.

Análisis

De la información anterior, podemos indicar que mayoría de los consultados señalaron que el grado de eficiencia y eficacia tienen concordancia con los resultados obtenidos con la empresa; es decir, que ante un mejor grado de eficiencia y eficacia en las operaciones de la empresa favorecen a los resultados.

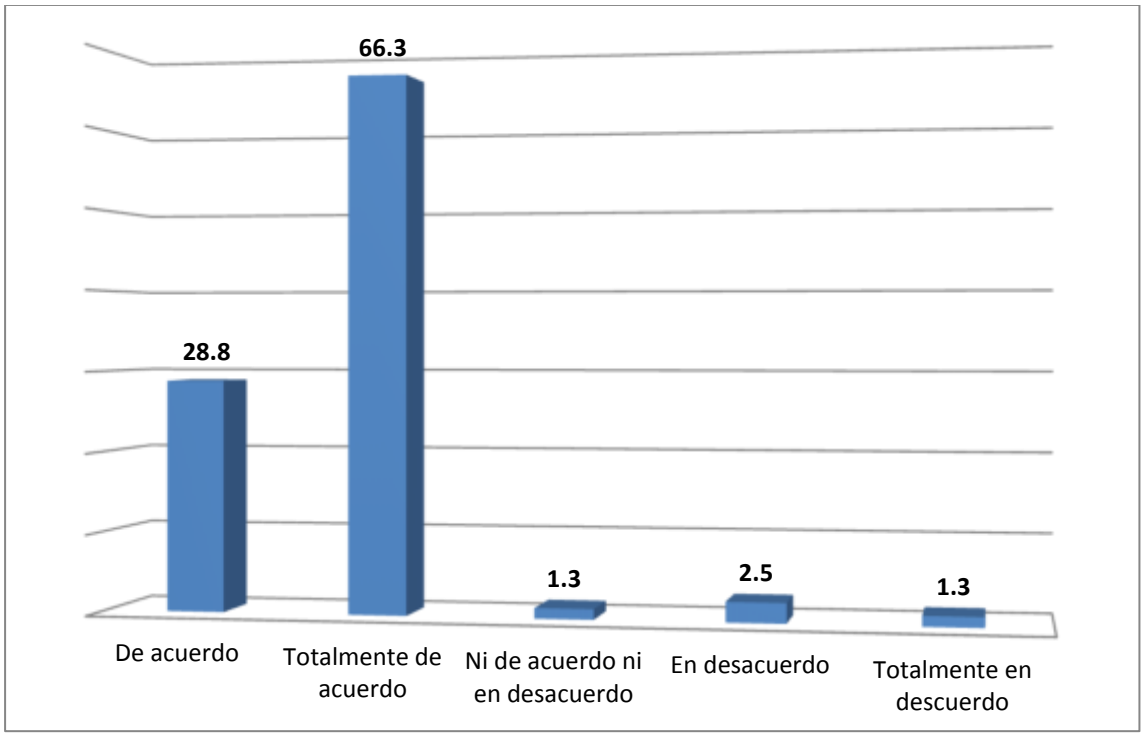

Figura 12. El grado de eficiencia y eficacia tienen concordancia con los resultados obtenidos por las empresas

Fuente. Tabla N° 12

5.1.13 Políticas y Normas de la Seguridad de Información en las empresas

Pregunta N° 13 - ¿Cree usted, que las políticas y normas de la seguridad de información, es óptimo en las empresas?

TABLA N°13

Alternativas	Auditores y funcionarios	Porcentaje
De acuerdo	28	35,0
Totalmente de acuerdo	49	61,3
Ni de acuerdo ni en desacuerdo	2	2,5
En desacuerdo	1	1,3
Totalmente en descuerdo	0	0,0
Total	80	100.0

Interpretación

La mayoría de Auditores y funcionarios de las empresas de Servicios Logísticos en la Provincia Constitucional del Callao como el 61,3%, manifestó estar totalmente de acuerdo que las políticas y normas de la seguridad de información, es óptimo en las empresas, mientras que otro porcentaje mínimo, 1,3%, de funcionarios y auditores manifestaron estar en desacuerdo que las políticas y normas de la seguridad de información, sea óptimo en las empresas.

Análisis

De la información anterior, podemos indicar que mayoría de los consultados señalaron que políticas y normas de la seguridad de información son óptimas en las empresas; es decir, que al aplicarlas adecuadamente mejoran en el desarrollo de las empresas.

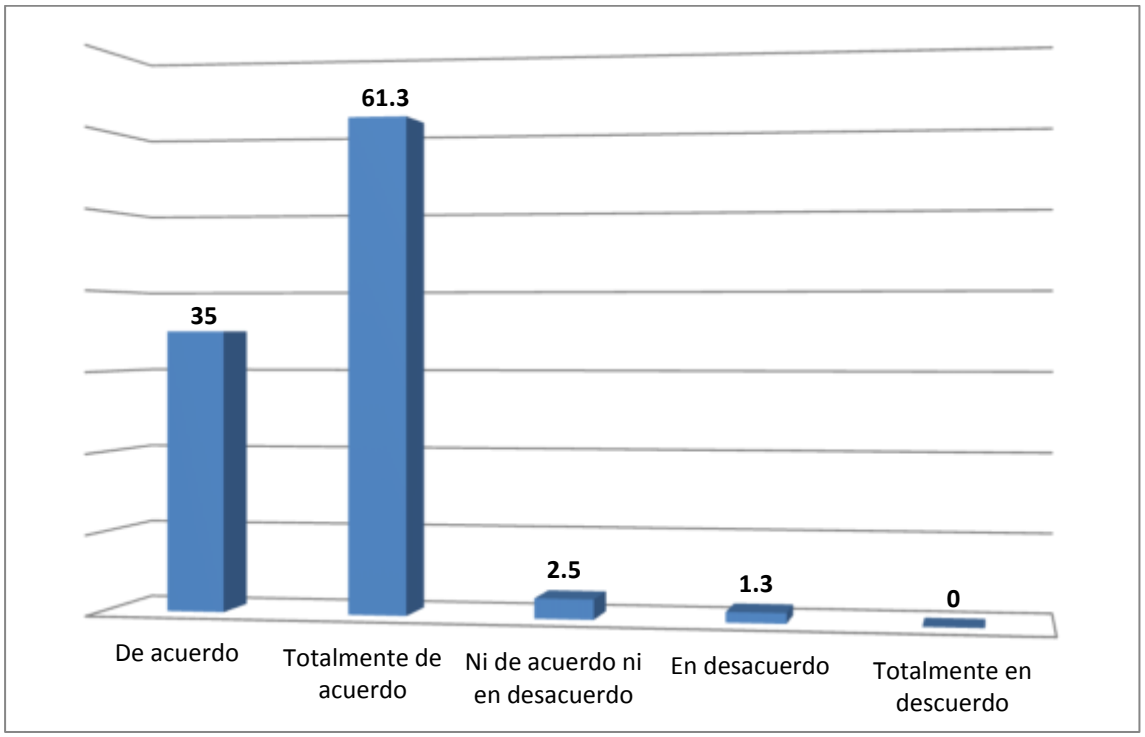

Figura 13. Las políticas y normas de la seguridad de información, es óptimo en las empresas

Fuente. Tabla N°13

5.1.14 La Gestión de Seguridad de la Información en las Empresas de Servicios Logísticos

Pregunta N° 14 - ¿La gestión de seguridad de la información es la adecuada en las Empresas de servicios logísticos?

TABLA N°14

Alternativas	Auditores y funcionarios	Porcentaje
De acuerdo	27	33,8
Totalmente de acuerdo	50	62,5
Ni de acuerdo ni en desacuerdo	1	1,3
En desacuerdo	2	2,5
Totalmente en descuerdo	0	0,0
Total	80	100.0

Interpretación

La seguridad es un factor importante dentro de las actividades empresariales, en especial de las empresas de Servicios Logísticos en la Provincia Constitucional del Callao. En ese sentido, el 62,5% de Auditores y funcionarios de estas empresas del Callao afirmó estar totalmente de acuerdo que la gestión de seguridad de la información es la adecuada, mientras que otro porcentaje mínimo, 2,5%, de funcionarios y auditores manifestaron estar en desacuerdo que la gestión de seguridad de la información sea la adecuada.

Análisis

De la información anterior, podemos indicar que mayoría de los consultados señalaron que la gestión de seguridad de la información es adecuada en las empresas de servicios logísticos; es decir, que contribuyen a salvaguardar los activos de información.

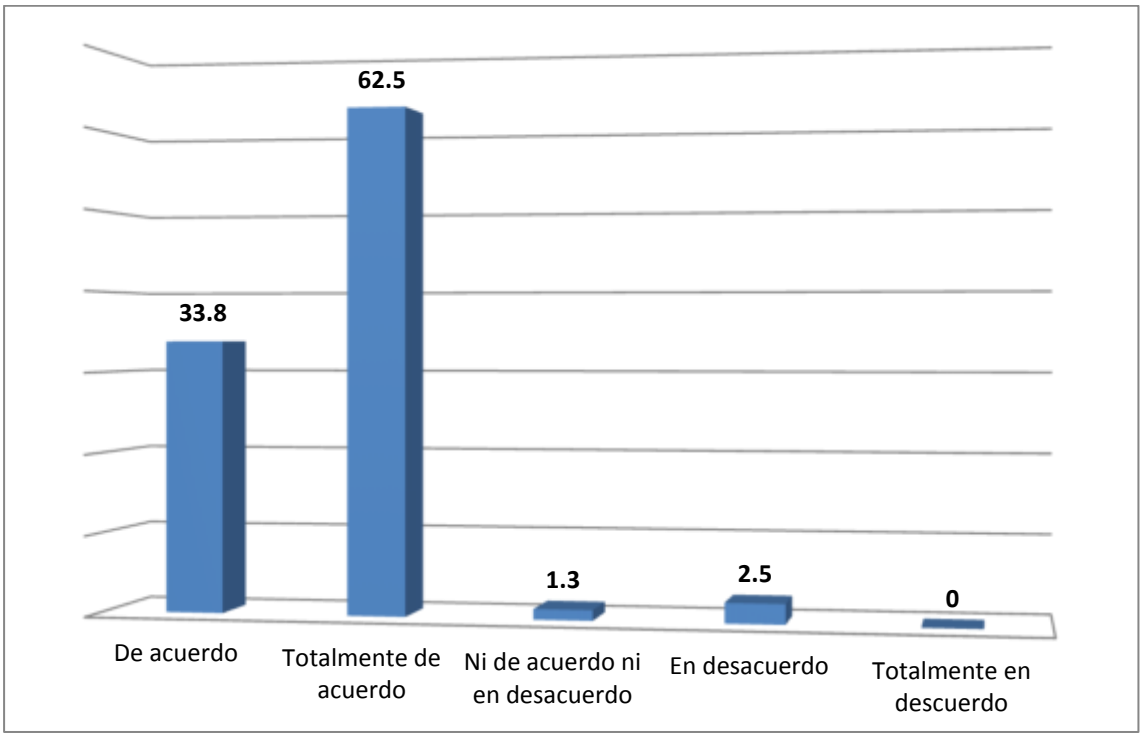

Figura 14. La gestión de seguridad de la información es la adecuada en las empresas de servicios logísticos

Fuente. Tabla N° 14

5.2 Contrastación de hipótesis

Para la contrastación de hipótesis se utilizó la prueba de Rangos señalados y pares igualados de Wilcoxon debido a la presencia de puntajes de diferencia de dos muestras relacionadas, es decir los auditores y funcionarios de las empresas servicios logísticos de la Provincia Constitucional del Callao constituyeron su propio control. Asimismo, las respuestas están medidas ordinalmente.

Hipótesis 1:

H_0 : El grado de independencia y objetividad no incide adecuadamente en el plan de seguridad de la información de los usuarios del sistema SAP.

H_1: El grado de independencia y objetividad incide adecuadamente en el plan de seguridad de la información de los usuarios del sistema SAP.

Existe Independencia y Objetividad	Existe Plan de Seguridad de la Información de los usuarios del sistema SAP					Total
	De acuerdo	Totalmente de acuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Totalmente en descuerdo	
De acuerdo	3	7	0	0	0	10
Totalmente de acuerdo	21	41	0	0	0	62
Ni de acuerdo ni en desacuerdo	1	4	1	0	0	6
En desacuerdo	0	0	1	0	0	1
Totalmente en descuerdo	0	0	0	1	0	1
Total	**25**	**52**	**2**	**1**	**0**	**80**

1. Estadística de prueba: Se escoge la prueba de Rangos señalados y pares igualados de Wilcoxon debido a la presencia de puntajes de diferencia de dos muestras relacionadas, donde cada sujeto es su propio control.

$$Z = \frac{T - \frac{n(n+1)}{4}}{\sqrt{\frac{n(n+1)(2n+1)}{24}}}$$

Donde:

T : Suma más pequeña de los rangos señalados.

n: muestra optima y a la vez el número de pares.

2. Nivel de significancia: sean $\alpha = 0.05$; n= 80

3. Regla de decisión: A un nivel de significancia de 0.05, Rechazar hipótesis nula (Ho) si la probabilidad asociada a Z; p < α .

4. Cálculo de la estadística de prueba. Al "correr" el SPSS con los datos sobre Liderazgo transformacional y desarrollar la fórmula a través del SPSS tenemos:

Estadísticos de contraste[a]

Estadísticos de Prueba	IO - PSI
Z	-3,569[b]
Sig. asintót. (bilateral)	,000

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

$$Z = \frac{T - \frac{80 * (80 + 1)}{4}}{\sqrt{\frac{80 * (80 + 1)(2 * 80 + 1)}{24}}} = -3,569$$

5. Decisión estadística: Dado que la probabilidad asociada a Z es p= 0,000 < 0.05 se Rechaza Ho.

6. Conclusión: El grado de independencia y objetividad incide adecuadamente en el plan de seguridad de la información de los usuarios del sistema SAP.

Hipótesis 2:

H_0 : El nivel de aporte de valor agregado no incide satisfactoriamente en el logro de los objetivos y metas de la Gestión de Seguridad de la información de los usuarios del sistema SAP.

H_1: El nivel de aporte de valor agregado incide satisfactoriamente en el logro de los objetivos y metas de la Gestión de Seguridad de la información de los usuarios del sistema SAP.

Existe Valor Agregado en las recomendaciones	Logra los Objetivos y Metas de la Gestión de Seguridad de la información de los usuarios del sistema SAP					Total
	De acuerdo	Totalmente de acuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Totalmente en descuerdo	
De acuerdo	4	8	0	0	0	12
Totalmente de acuerdo	25	40	0	1	0	66
Ni de acuerdo ni en desacuerdo	0	0	1	0	0	1
En desacuerdo	0	0	0	1	0	1
Totalmente en descuerdo	0	0	0	0	0	0
Total	**29**	**48**	**1**	**2**	**0**	**80**

1. Estadística de prueba: Se escoge la prueba de Rangos señalados y pares igualados de Wilcoxon debido a la presencia de puntajes de diferencia de dos muestras relacionadas, donde cada sujeto es su propio control.

$$Z = \frac{T - \frac{n(n+1)}{4}}{\sqrt{\frac{n(n+1)(2n+1)}{24}}}$$

Donde:

T : Suma más pequeña de los rangos señalados.

n: muestra optima y a la vez el número de pares.

2. Nivel de significancia: sean $\alpha = 0.05$; n= 80

3. Regla de decisión: A un nivel de significancia de 0.05, Rechazar hipótesis nula (Ho) si la probabilidad asociada a Z; p < α .

4. Cálculo de la estadística de prueba. Al “correr” el SPSS con los datos sobre Liderazgo transformacional y desarrollar la fórmula a través del SPSS tenemos:

Estadísticos de contraste[a]

Estadísticos de Prueba	VAR - OM
Z	-2,466[b]
Sig. asintót. (bilateral)	,014

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

$$Z = \frac{T - \frac{80 * (80 + 1)}{4}}{\sqrt{\frac{80 * (80 + 1)(2 * 80 + 1)}{24}}} = -2,466$$

5. Decisión estadística: Dado que la probabilidad asociada a Z es p= 0.014 < 0.05 se Rechaza Ho.

6. Conclusión: El nivel de aporte de valor agregado incide satisfactoriamente en el logro de los objetivos y metas de la Gestión de Seguridad de la información de los usuarios del sistema SAP.

Hipótesis 3:

H_0 : El nivel del sistema de control interno no incide adecuadamente en el grado de aceptación del riesgo de la organización en la Gestión de Seguridad de la información de los usuarios del sistema SAP.

H_1: El nivel del sistema de control interno incide adecuadamente en el grado de aceptación del riesgo de la organización en la Gestión de Seguridad de la información de los usuarios del sistema SAP.

Existe Evaluación del sistema de Control Interno	Grado de aceptación del riesgo de la organización en la Gestión de Seguridad de la Información de los usuarios del sistema SAP					Total
	De acuerdo	Totalmente de acuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Totalmente en descuerdo	
De acuerdo	4	6	0	0	0	10
Totalmente de acuerdo	23	45	0	0	0	68
Ni de acuerdo ni en desacuerdo	0	0	0	1	0	1
En desacuerdo	0	0	0	1	0	1
Totalmente en descuerdo	0	0	0	0	0	0
Total	**27**	**51**	**0**	**2**	**0**	**80**

1. Estadística de prueba: Se escoge la prueba de Rangos señalados y pares igualados de Wilcoxon debido a la presencia de puntajes de diferencia de dos muestras relacionadas, donde cada sujeto es su propio control.

$$Z = \frac{T - \frac{n(n+1)}{4}}{\sqrt{\frac{n(n+1)(2n+1)}{24}}}$$

Donde:

T : Suma más pequeña de los rangos señalados.

n: muestra optima y a la vez el número de pares.

2. Nivel de significancia: sean $\alpha = 0.05$; n= 80

3. Regla de decisión: A un nivel de significancia de 0.05, Rechazar hipótesis nula (Ho) si la probabilidad asociada a Z; p < α .

4. Cálculo de la estadística de prueba. Al “correr” el SPSS con los datos sobre Liderazgo transformacional y desarrollar la fórmula a través del SPSS tenemos:

Estadísticos de contraste[a]

Estadísticos de Prueba	ESCI - GARO
Z	-2,921[b]
Sig. asintót. (bilateral)	,003

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

$$Z = \frac{T - \frac{80 * (80 + 1)}{4}}{\sqrt{\frac{80 * (80 + 1)(2 * 80 + 1)}{24}}} = -2{,}921$$

5. Decisión estadística: Dado que la probabilidad asociada a Z es p= 0.003 < 0.05 se Rechaza Ho.

6. Conclusión: El nivel del sistema de control interno incide adecuadamente en el grado de aceptación del riesgo de la organización en la Gestión de Seguridad de la información de los usuarios del sistema SAP.

Hipótesis 4:

H_0 : Las acciones de control no inciden en la efectividad de las operaciones de la Gestión de Seguridad de la información de los usuarios del sistema SAP.

H_1: Las acciones de control inciden en la efectividad de las operaciones de la Gestión de Seguridad de la información de los usuarios del sistema SAP.

Existen Acciones de Control	Existe efectividad de las operaciones de la Gestión de Seguridad de la información de los usuarios del sistema SAP					Total
	De acuerdo	Totalmente de acuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Totalmente en descuerdo	
De acuerdo	6	12	0	0	0	18
Totalmente de acuerdo	23	36	0	1	0	60
Ni de acuerdo ni en desacuerdo	0	0	0	1	0	1
En desacuerdo	0	0	0	0	1	1
Totalmente en descuerdo	0	0	0	0	0	0
Total	**29**	**48**	**0**	**2**	**1**	**80**

1. Estadística de prueba: Se escoge la prueba de Rangos señalados y pares igualados de Wilcoxon debido a la presencia de puntajes de diferencia de dos muestras relacionadas, donde cada sujeto es su propio control.

$$Z = \frac{T - \frac{n(n+1)}{4}}{\sqrt{\frac{n(n+1)(2n+1)}{24}}}$$

Donde:

T : Suma más pequeña de los rangos señalados.

n: muestra optima y a la vez el número de pares.

2. Nivel de significancia: sean $\alpha = 0.05$; n= 80

3. Regla de decisión: A un nivel de significancia de 0.05, Rechazar hipótesis nula (Ho) si la probabilidad asociada a Z; p < α .

4. Cálculo de la estadística de prueba. Al “correr” el SPSS con los datos sobre Liderazgo transformacional y desarrollar la fórmula a través del SPSS tenemos:

Estadísticos de contraste[a]

Estadísticos de Prueba	AC – EOGS
Z	-7,575[b]
Sig. asintót. (bilateral)	,000

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

$$Z = \frac{T - \frac{80 * (80 + 1)}{4}}{\sqrt{\frac{80 * (80 + 1)(2 * 80 + 1)}{24}}} = -7{,}575$$

5. Decisión estadística: Dado que la probabilidad asociada a Z es p= 0,000 < 0.05 se Rechaza Ho.

6. Conclusión: Las acciones de control inciden en la efectividad de las operaciones de la Gestión de Seguridad de la información de los usuarios del sistema SAP.

Hipótesis 5:

H_0 : El seguimiento de las recomendaciones no incide satisfactoriamente en el grado de eficiencia y eficacia de la Gestión de Seguridad de la información de los usuarios del sistema SAP.

H_1: El seguimiento de las recomendaciones incide satisfactoriamente en el grado de eficiencia y eficacia de la Gestión de Seguridad de la información de los usuarios del sistema SAP.

Existe un seguimiento de las recomendaciones	Existe eficiencia y eficacia de la Gestión de Seguridad de la información de los usuarios del sistema SAP					Total
	De acuerdo	Totalmente de acuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Totalmente en descuerdo	
De acuerdo	5	9	0	0	0	14
Totalmente de acuerdo	18	44	1	1	0	64
Ni de acuerdo ni en desacuerdo	0	0	0	1	0	1
En desacuerdo	0	0	0	0	1	1
Totalmente en descuerdo	0	0	0	0	0	0
Total	**23**	**53**	**1**	**2**	**1**	**80**

1. Estadística de prueba: Se escoge la prueba de Rangos señalados y pares igualados de Wilcoxon debido a la presencia de puntajes de diferencia de dos muestras relacionadas, donde cada sujeto es su propio control.

$$Z = \frac{T - \frac{n(n+1)}{4}}{\sqrt{\frac{n(n+1)(2n+1)}{24}}}$$

Donde:

T : Suma más pequeña de los rangos señalados.

n: muestra optima y a la vez el número de pares.

2. Nivel de significancia: sean $\alpha = 0.05$; n= 80

3. Regla de decisión: A un nivel de significancia de 0.05, Rechazar hipótesis nula (Ho) si la probabilidad asociada a Z; p < α .

4. Cálculo de la estadística de prueba. Al “correr” el SPSS con los datos sobre Liderazgo transformacional y desarrollar la fórmula a través del SPSS tenemos:

Estadísticos de contraste[a]

Estadísticos de Prueba	SR - EEG
Z	-7,661[b]
Sig. asintót. (bilateral)	,000

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

$$Z = \frac{T - \frac{80 * (80 + 1)}{4}}{\sqrt{\frac{80 * (80 + 1)(2 * 80 + 1)}{24}}} = -7,661$$

5. Decisión estadística: Dado que la probabilidad asociada a Z es p= 0,000< 0.05 se Rechaza Ho.

6. Conclusión: El seguimiento de las recomendaciones incide satisfactoriamente en el grado de eficiencia y eficacia de la Gestión de Seguridad de la información de los usuarios del sistema SAP.

Hipótesis 6:

H_0: Los informes de auditoría no incide razonablemente en el fortalecimiento de las políticas y normas de la seguridad de la información de los usuarios del sistema SAP.

H_1: Los informes de auditoría incide razonablemente en el fortalecimiento de las políticas y normas de la seguridad de la información de los usuarios del sistema SAP.

Los Informes de Auditoría contribuyen en el desarrollo de la Gestión de Seguridad	Existe fortalecimiento de las políticas y normas de la seguridad de la información de los usuarios del sistema SAP					Total
	De acuerdo	Totalmente de acuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Totalmente en descuerdo	
De acuerdo	3	9	0	0	0	12
Totalmente de acuerdo	25	40	1	0	0	66
Ni de acuerdo ni en desacuerdo	0	0	1	0	0	1
En desacuerdo	0	0	0	1	0	1
Totalmente en descuerdo	0	0	0	0	0	0
Total	**28**	**49**	**2**	**1**	**0**	**80**

1. Estadística de prueba: Se escoge la prueba de Rangos señalados y pares igualados de Wilcoxon debido a la presencia de puntajes de diferencia de dos muestras relacionadas, donde cada sujeto es su propio control.

$$Z = \frac{T - \frac{n(n+1)}{4}}{\sqrt{\frac{n(n+1)(2n+1)}{24}}}$$

Donde:

T : Suma más pequeña de los rangos señalados.

n: muestra optima y a la vez el número de pares.

2. Nivel de significancia: sean $\alpha = 0.05$; n= 80

3. Regla de decisión: A un nivel de significancia de 0.05, Rechazar hipótesis nula (Ho) si la probabilidad asociada a Z; p < α .

4. Cálculo de la estadística de prueba. Al “correr” el SPSS con los datos sobre Liderazgo transformacional y desarrollar la fórmula a través del SPSS tenemos:

Estadísticos de contraste[a]

Estadísticos de Prueba	IA - FPNS
Z	-7,762[b]
Sig. asintót. (bilateral)	,000

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

$$Z = \frac{T - \frac{80 * (80 + 1)}{4}}{\sqrt{\frac{80 * (80 + 1)(2 * 80 + 1)}{24}}} = -7{,}762$$

5. Decisión estadística: Dado que la probabilidad asociada a Z es p= 0,000 < 0.05 se Rechaza Ho.

6. Conclusión: Los informes de auditoría incide razonablemente en el fortalecimiento de las políticas y normas de la seguridad de la información de los usuarios del sistema SAP.

Hipótesis General:

H_0 : La Auditoría Interna no incide favorablemente en la optimización de la Gestión de Seguridad de la información de los usuarios del sistema SAP en empresas de servicios logísticos de la Provincia Constitucional del Callao, año 2016-2017.

H_1: La Auditoría Interna incide favorablemente en la optimización de la Gestión de Seguridad de la información de los usuarios del sistema SAP en empresas de servicios logísticos de la Provincia Constitucional del Callao, año 2016-2017.

Existe Auditoría Interna	Existe optimización de la Gestión de Seguridad de la Información de los usuarios SAP en las empresas de servicios logísticos					Total
	De acuerdo	Totalmente de acuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Totalmente en descuerdo	
De acuerdo	12	1	0	0	0	13
Totalmente de acuerdo	15	48	1	0	0	64
Ni de acuerdo ni en desacuerdo	0	1	0	1	0	2
En desacuerdo	0	0	0	1	0	1
Totalmente en descuerdo	0	0	0	0	0	0
Total	**27**	**50**	**1**	**2**	**0**	**80**

1. Estadística de prueba: Se escoge la prueba de Rangos señalados y pares igualados de Wilcoxon debido a la presencia de puntajes de diferencia de dos muestras relacionadas, donde cada sujeto es su propio control.

$$Z = \frac{T - \frac{n(n+1)}{4}}{\sqrt{\frac{n(n+1)(2n+1)}{24}}}$$

Donde:

T : Suma más pequeña de los rangos señalados.

n: muestra optima y a la vez el número de pares.

2. Nivel de significancia: sean $\alpha = 0.05$; n= 80
3. Regla de decisión: A un nivel de significancia de 0.05, Rechazar hipótesis nula (Ho) si la probabilidad asociada a Z; p < α .

4. Cálculo de la estadística de prueba. Al “correr” el SPSS con los datos sobre Liderazgo transformacional y desarrollar la fórmula a través del SPSS tenemos:

Estadísticos de contraste[a]

Estadísticos de Prueba	AI - OGSI
Z	-2,982[b]
Sig. asintót. (bilateral)	,003

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

$$Z = \frac{T - \frac{80 * (80 + 1)}{4}}{\sqrt{\frac{80 * (80 + 1)(2 * 80 + 1)}{24}}} = -2{,}982$$

5. Decisión estadística: Dado que la probabilidad asociada a Z es p= 0.003 < 0.05 se Rechaza Ho.

6. Conclusión: La Auditoría Interna incide favorablemente en la optimización de la Gestión de Seguridad de la información de los usuarios del sistema SAP en empresas de servicios logísticos de la Provincia Constitucional del Callao, año 2016-2017.

CAPITULO VI

DISCUSION, CONCLUSIONES Y RECOMENDACIONES

6.1. Discusión

De acuerdo a los resultados obtenidos en la aplicación del instrumento, podemos indicar que entre otros existen algunos resultados que son relevantes para la investigación y que deben ser tomados en cuenta:

- Respecto a que las labores de Auditoría Interna se realicen con un grado de independencia y objetividad en las empresas de servicios logísticos en el Callao, esta opción fue aceptada en forma mayoritaria, señalando que la labor del auditor interno es imparcial en la comunicación de sus hallazgos y recomendaciones, esto contribuye en una adecuada toma de decisiones de la alta Gerencia y en los Comités de Auditoría. (77.50%, tabla 1).

- Respecto a la información obtenida, los encuestados indicaron que si es importante las recomendaciones de Auditoría Interna porque agregan valor a las operaciones de las empresas de servicios logísticos en el Callao, esto se sustenta a que el Auditor Interno evalúa el cumplimiento de los controles existentes y sugiere nuevos controles para los

principales procesos de las empresas logísticas, tales como: almacenamiento, distribución y transportes de las mercaderías secas y fríos. (82.50%, tabla 2).

- Del mismo modo, se estableció la necesidad de que el Auditor evalúe el nivel de sistema de control interno de las empresas de servicios logísticos en el Callao, esta opción fue aceptada en forma mayoritaria, debido a que el Auditor evalúa el cumplimiento de las normas, políticas y procedimientos establecidos, realizándose de forma sorpresiva e inopinada, visitando las instalaciones de las empresas, como los servicios onsite que se brindan dentro de las instalaciones de los clientes logísticos. (85% tabla 3).

- También se logró obtener como resultado mayoritario que las acciones de control contenidas en el plan anual se aplican en las empresas de servicios logísticos en el Callao, lo que permite que el área de Auditoría Interna identifique y evalúe los riesgos relacionados a los procesos auditados en los negocios de las empresas, poniendo mayor y especial énfasis sobre los riesgos en los sectores de Consumo Masivo, Industrial, Minería, Gas y Petróleo, siendo más relevantes y de mayor criticidad para las empresas logísticas. (75% tabla 4)

- En lo que se refiere al seguimiento de las recomendaciones de Auditoría Interna contenidas en los Informes, si constituye una herramienta de gestión para la mejora de las empresas, los resultados muestran que la mayoría se encuentra totalmente de acuerdo, debido que las recomendaciones de Auditoría Interna impactan favorablemente a los negocios logísticos, a través del mejoramiento continuo y el desarrollo de estrategias para un adecuado sistema de control interno. (80% tabla 5).

- Asimismo, se sostuvo que los informes de Auditoría contribuyen en la gestión de las empresas de servicios logísticos; es decir, que con dicha información aporta observaciones y recomendaciones que contribuyen en

alcanzar los objetivos de las empresas, tales como: optimización de las condiciones de almacenamiento, control de pesaje en el ingreso y salidas de las mercaderías, liquidación de servicios de transportes con flota propia y tercera, validar que los servicios brindados a los clientes sean facturados en su totalidad y evaluar la rentabilidad obtenida por las operaciones logísticas de sus clientes. (82.50% tabla 6).

- Del mismo modo, se obtuvieron datos favorables indicando que la función de Auditoría Interna cumple un papel importante en las empresas de servicios logísticos en el Callao, debido que al ser considerada como una actividad de evaluación independiente contribuyen en el fortalecimiento de los procesos, políticas y procedimiento dentro de las empresas logísticas, manteniendo una comunicación permanente con la Alta Gerencia sobre la ocurrencia de hechos de relevancia de alto riesgo e impacto para las empresas de servicios logísticos. (78.80% tabla 7).

- Respecto a los resultados que se obtuvieron sobre si lo Planes de Seguridad aportan en la prevención de los riesgos empresariales en las empresas de servicios logísticos en el Callao, esto permitió conocer que la mayoría se encuentra de acuerdo; es decir, que los Planes de Seguridad sirven como una herramienta de control, la cual permite establecer los riesgos asociados y establecer acciones que minimicen los riesgos de la información de los sistemas operativos que utilizan las empresas de servicios logísticos. (65% tabla 8).

- De otro lado, se obtuvieron resultados favorables sobre la importancia del logro de los objetivos y metas en las empresas de servicios logísticos, que permite el desarrollo y gestión de la seguridad de la información, debiendo preservar la confiabilidad, integridad y disponibilidad de la información sensible de las empresas de servicios logísticos (60% tabla 9).

- También se logró un resultado mayoritario respecto que efectivamente el grado de aceptación es manejable o administrable utilizándose en las empresas de servicios logísticos en el Callao; es decir, ayudan a las empresas a identificar, evaluar e implantar metodologías de gestión de riesgos y controles para tratar aquellos riesgos aceptados, debiendo ser justificados por las Gerencias, estableciendo las acciones y frecuencias de los controles que mitiguen el riesgo residual. (63.80% tabla 10).

- En cuanto que la efectividad de las operaciones son reportadas de manera sustentada en la empresa, el presente estudio nos permite conocer que la mayoría, coincidieron en estar de acuerdo, debido a que esta información se basa de indicadores de gestión que deben ser utilizados por las empresas de servicios logísticos en las operaciones de sus clientes, tales como: metros cuadros de almacenamiento, número de posiciones, número de posiciones con temperatura controlada, recorrido de unidades con GPS, etc. (60% tabla 11).

- Del mismo modo, obtuvimos como resultado mayoritario que el grado de eficiencia y eficacia tienen concordancia con los resultados de las empresas de servicios logísticos en el Callao; es decir, que ante un mejor grado de eficiencia y eficacia en las operaciones de la empresa favorecen a los resultados, convirtiéndose en una ventaja competitiva para integrar la cadena logística de sus clientes con servicios desde transporte, almacenamiento y distribución, hasta los de valor agregado como empaque, maquila o seguimiento de carga. (66.30% tabla 12).

- En cuanto a las políticas y normas de la seguridad de información en las empresas de servicios logísticos, el presente estudio nos permite conocer que la mayoría de los encuestados se encuentran de acuerdo, esto se sustenta con la necesidad de aplicar buenas prácticas en el control de los accesos de los usuarios SAP, a fin de minimizar el riesgo de su mal uso y asegurando la continuidad de las operaciones en las empresas de servicios logísticos. (61.3% tabla 13).

- Respecto a la gestión de seguridad de la información en las empresas de servicios logísticos en el Callao, el presente estudio nos permite conocer que la mayoría respondieron afirmativamente, esto permite que existan adecuados controles para los cambios en los accesos de los usuarios y la utilización de transacciones del sistema SAP, otorgados de acuerdo a sus funciones que desempeñan los colaboradores en las empresas logísticas. (62.50% tabla 14).

6.2. Conclusiones

Culminada la investigación, se llegaron a las siguientes conclusiones:

1. Se ha determinado que el grado de independencia y objetividad incide adecuadamente en el plan de seguridad de la información de los usuarios del sistema SAP, con la participación del auditor de manera imparcial.

2. Como producto del análisis de los datos se ha establecido que el nivel de aporte de valor agregado incide satisfactoriamente en el logro de los objetivos y metas de la Gestión de Seguridad de la información de los usuarios del sistema SAP, cooperando en la mejora continua de las empresas.

3. El análisis de los datos ha permitido establecer que el nivel del sistema de control interno incide adecuadamente en el grado de aceptación del riesgo de la organización en la Gestión de Seguridad de la información de los usuarios del sistema SAP, evaluando los riesgos de las empresas.

4. Se ha demostrado que las acciones de control inciden en la efectividad de las operaciones de la Gestión de Seguridad de la información de los usuarios del sistema SAP, impulsando el cumplimiento de las normas y procedimientos establecidos.

5. Se ha comprobado que el seguimiento de las recomendaciones incide satisfactoriamente en el grado de eficiencia y eficacia de la Gestión de Seguridad de la información de los usuarios del sistema SAP, potenciando los controles en las empresas.

6. Como producto del análisis de los datos se ha establecido que los informes de auditoría inciden razonablemente en el fortalecimiento de las políticas y normas de la seguridad de la información de los usuarios del sistema SAP, mejorando los niveles de gestión en las empresas.

7. **Conclusión General**: La prueba de la hipótesis ha permitido determinado que la Auditoría Interna incide favorablemente en la optimización de la Gestión de Seguridad de la información de los usuarios del sistema SAP en empresas de servicios logísticos de la Provincia Constitucional del Callao, año 2016-2017, contribuyendo en la identificación de los riesgos en las empresas.

6.3. Recomendaciones

En virtud a las conclusiones precedentes se estima formular las siguientes recomendaciones:

1. Es importante que la función de Auditoría Interna desarrolle su labor en las empresas de servicios logísticos de la Provincia Constitucional del Callao con un grado óptimo de independencia y objetividad, esto contribuirá a una mejor planificación de las actividades a ejecutar en el programa de Auditoría, con el propósito de evaluar el cumplimiento de los planes y/o políticas de seguridad de la información de los usuarios del sistema SAP.

2. Es necesario que las empresas de servicios logísticos de la Provincia Constitucional del Callao, consideren el nivel de aporte de valor agregado que brinda Auditoría Interna, el cual proporciona recomendaciones apropiadas para la mejora de los procesos de las organizaciones, debido a su conocimiento y visión integradora de los negocios, los cuales se respaldan con el logro de los objetivos y metas establecidos en la Gestión de Seguridad de la información de los usuarios SAP, debiendo identificar los riesgos a los que se encuentra expuesta la información sensible y éstas sean asumidas, gestionadas y minimizadas por las organizaciones.

3. Se recomienda que las empresas de servicios logísticos establezcan un nivel adecuado del sistema de control interno, debiendo encontrarse documentada y estructurada, con el propósito de dar una respuesta inmediata a los cambios que se produzcan en los riesgos, el entorno y las tecnologías; asimismo, evaluar el grado de aceptación del riesgo inherente en la Gestión de Seguridad de la información de los usuarios SAP, de manera de reducir a un nivel aceptable para el negocio, controlando que los accesos al sistema SAP sean asignados y actualizados de acuerdo a las actividades que realizan los colaboradores.

4. Es conveniente que las actividades o acciones de control que se ejecutan a los usuarios de sistema SAP de las empresas de servicios logísticos realizado por Auditoría Interna se evalúe el grado de efectividad en las operaciones de la Gestión de Seguridad de información, de manera que se pueda identificar los procesos o unidades relevantes donde puedan surgir errores materiales en sus perfiles de accesos.

5. Dada la importancia que tiene el seguimiento de las recomendaciones de Auditoría Interna para la Gestión de la Seguridad de la información de los usuarios del sistema SAP, es necesario que las áreas auditadas establezcan planes de acción respecto a las observaciones encontradas, con la finalidad que la Administración evalúe el grado de eficiencia y eficacia en el manejo de la seguridad de la información en las empresas.

6. Se sugiere que los informes de Auditoría Interna que son respaldados con evidencia suficiente, confiable y relevante que permite fundamentar opiniones, conclusiones y recomendaciones sirvan como insumo para el fortalecimiento de las políticas, procedimientos y normas en la Gestión de la Seguridad de la información de los usuarios del sistema SAP en las empresas de servicios logísticos.

7. Es conveniente que se optimice la Gestión de la Seguridad de la Información de los usuarios del sistema SAP a través de la Auditoría Interna en las empresas de servicios logísticos, a fin de lograr que se encuentren en capacidad de atender a los diferentes sectores como: Minería & Energía, Consumo Masivo & Retail, Industrias y logística refrigerada, con un sistema de control interno sólido y efectivo.

FUENTES DE INFORMACIÓN

REFERENCIAS BIBLIOGRÁFICAS

1. Aguilera Lopez, Purificación (2010). Seguridad Informática, España: Editorial Editex SA.

2. Alegre Maria Y García-Cervigón Alfonso (2011). Seguridad Informática, España: Ediciones Paraninfo.

3. Areitio Bertolin Javier (2008). Seguridad de la Información, España: Ediciones Paraninfo.

4. Arens, Alvin Y James Loebbecke (2010). Auditoría Un Enfoque Integral. México: Prentice Hall.

5. Argandoña, Marco Antonio (2010). Nuevo Enfoque de la Auditoría Financiera, Presupuestal y de Gestión Gubernamental, Perú, Marketing y Consultores SA.

6. Asap World Consultancy y Jonathan Blain (1999). Edición Especial SAP R/3, Estados Unidos: Editorial Pretience Hall.

7. Baca Urbina, Gabriel (2016). Introducción a la Seguridad Informática, México: Grupo Editorial Patria.

8. Borrajo Dominguez Manuel (2002). La Auditoría Externa e Interna, España: Partida Doble.

9. Cashin, James, Neuwirth Paul y Levy John (1985). Manual de Auditoría, España: Ediciones Centrum Técnicas y Científicas.

10. David Coderre (2005). Guía de Auditoría de Tecnología Global-GTAG, Auditoría Continúa: Implicancias para el Aseguramiento, Supervisión y la Evaluación de Riesgos, Estados Unidos: Instituto de Auditores Internos.

11. David Richards, Alan y Charles Le Grand (2005). GTAC-Guía de Auditoría de Tecnología Global del IAI-Controles de Tecnología de Información, Estados Unidos, Instituto de Auditores Internos.

12. Editorial Océano (2011). Enciclopedia de la Auditoría Interna, España: Océano Centrum.

13. Estupiñan, Rodrigo (2015). Administración de Riesgos ERM y la Auditoria Interna, Colombia: Ecoe Ediciones.

14. Godoy Lemus, Rodolfo (2014). Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica, Guatemala: Universidad de San Carlos de Guatemala.

15. Gomez Vieites, Alvaro (2014). Enciclopedia de la Seguridad Informática, España: Editorial Ra-Ma.

16. Gutierrez Jaime y Juan Tena (2003). Protocolos Criptográficos y Seguridad En Redes, España: Graficas Calima.

17. Haberkorn, Ernesto (2003). Gestión Empresarial Con ERP, Brasil: Editorial Microsiga SA Company.

18. Hernandez Muñoz Jose (1998). Así es SAP R/3, España: Editorial Mcgraw Hill.

19. Hernandez Muñoz Jose (2000). Implementación de SAP R/3, España: Editorial M Mcgraw Hill.

20. Hernandez Muñoz Jose (2000). Manual de SAP R/3, España, Editorial Mcgraw Hill.

21. Instituto de Auditores Internos de España (2013). Marco Internacional para la Práctica Profesional de la Auditoría Interna, España: Alba SA.

22. Instituto Latinoamericano de Ciencias Fiscalizadoras (1981). Auditoría Interna, Colombia: Editorial Dintel Ltda.

23. Ley N°28951 de actualización de la Ley N° 13253 de Profesionalización del Contador Público y de Creación de los Colegios de Contadores Públicos (2007). Perú: Diario Oficial El Peruano.

24. Ley que Modifica el Artículo 366 de la Ley N°26702, incorpora una disposición final y complementaria, Modifica los artículos 198, 244 y 245 del Código Penal (2006). Perú: Diario Oficial El Peruano.

25. Madariaga Gorocica, Juan (2004). Manual Práctico de Auditoría, España: Ediciones Deusto.

26. Montesinos Vicente (1992) La Auditoría en España, España: Universidad de Valencia.

27. Morales, Juan Carlos (2017). Dirección Eficaz de Tecnología de la Información, Estados Unidos: Smashwords Edition.

28. Nudman Puyol (2008). Manual De Auditoría Operativa, España: Editorial Mcgraw-Hill.

29. Pardo Vega, Julio (2009). Fundamentos de Auditoría Administrativa, Perú: Editorial Desarrollo.

30. Ramio Aguirre, Jorge (2006). Seguridad Informática, España: Editorial Eui-Upm Company.

31. Rusenas, Rubén (1999). Manual de Auditoría Interna y Operativa, Argentina: Editorial Cangallo.

32. Santillana, Juan (2005). Auditoría Interna Integral, México, Pearson.

33. Spencer Pickett (2007). Manual Básico de Auditoría Interna, España: Ediciones Gestión 2000.

34. Tapia Carmen, Rahell y Silva, Ricardo (2017). Auditoría Interna perspectiva de vanguardia, México: Instituto Mexicano de Contadores Públicos.

35. Universidad de Buenos Aires (2008). Manual de Auditoría Interna, Argentina: Editorial Universidad de Buenos Aires.

REFERENCIAS ELECTRÓNICAS

1. Instituto de Auditores Internos. Código de Ética. Extraído el 22 de abril 2018 desde http://iaiperu.org/publicaciones/normas-y-codigo-de-etica/

2. Informática Dinámica Universal. Historia de la Creación de Sistemas ERP. Extraído el 12 de abril 2018 desde http://idu-net.com/sistemas1.pdf/

3. PANORAMA CONSULTING GROUP. 2011 ERP Report. Extraído el 06 de enero 2018 desde http://panorama-consulting.com/erp-vendors/

4. WIKIPEDIA (2008). Seguridad de la Información, Recuperado de: https://es.wikipedia.org/wiki/Seguridad_de_la_información

ANEXOS

ANEXO N° 01 - MATRIZ DE CONSISTENCIA

LA AUDITORIA INTERNA Y SU INCIDENCIA EN LA OPTIMIZACIÓN DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACION DE LOS USUARIOS DEL SISTEMA SAP DE LAS EMPRESAS DE SERVICIOS LOGÍSTICOS EN LA PROVINCIA CONSTITUCIONAL DEL CALLAO, AÑO 2016-2017

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES	METODOLOGIA
1. Problema Principal ¿De qué manera la Auditoría Interna incide en la optimización de la Gestión de Seguridad de la información de los usuarios del sistema SAP en empresas de servicios logísticos de la Provincia Constitucional del Callao, año 2016-2017?	**1. Objetivo General** Determinar si la Auditoría Interna incide en la optimización de la Gestión de Seguridad de la información de los usuarios del sistema SAP en empresas de servicios logísticos de la Provincia Constitucional del Callao, año 2016-2017.	**1. Hipótesis Principal** La Auditoría Interna incide favorablemente en la optimización de la Gestión de Seguridad de la información de los usuarios del sistema SAP en empresas de servicios logísticos de la Provincia Constitucional del Callao, año 2016-2017, contribuyendo en la identificación de los riesgos en las empresas.	**1. Variable Independiente** **X: Auditoría Interna** **Indicadores** **X1.** Grado de independencia y objetividad. **X2.** Nivel de aporte de valor agregado a la empresa. X3. Evaluar nivel de Control Interno. X4. Acciones de control. X5. Seguimiento de recomendaciones. **X6.** Informes de Auditoría Interna. **2. Variable Dependiente** **Y: Gestión de Seguridad de la Información.** **Indicadores** **Y1.** Plan de Seguridad. **Y2.** Logro de Objetivos y Metas. **Y3.** Evaluar el grado de aceptación del riesgo de la organización. **Y4.** Efectividad de operaciones. **Y5.** Grado de eficiencia y eficacia. **Y6.** Fortalecimiento de las políticas y normas de la seguridad de la información.	**1. Tipo de Investigación** Aplicada **2. Nivel de Investigación** Descriptivo Explicativo **3. Población** 101 personas. **4. Muestra** 80 personas. **5. Técnicas e Instrumentos** Técnica: Encuesta Instrumento: Cuestionario
2. Problemas Secundarios	**2. Objetivos Específicos**	**2. Hipótesis Secundarias**		
a. De qué manera el grado de independencia y objetividad incide en el plan de seguridad de la información de los usuarios del sistema SAP?	a. Evaluar si el grado de independencia y objetividad incide en el plan de seguridad de la información de los usuarios del sistema SAP.	a. El grado de independencia y objetividad incide adecuadamente en el plan de seguridad de la información de los usuarios del sistema SAP, con la participación del auditor de manera imparcial.		
b. En qué medida el nivel de aporte de valor agregado incide en el logro de los objetivos y metas de la Gestión de Seguridad de la información de los usuarios del sistema SAP?	b. Establecer el nivel de aporte de valor agregado incide en el logro de los objetivos y metas de la Gestión de Seguridad de la información de los usuarios del sistema SAP.	b. El nivel de aporte de valor agregado incide satisfactoriamente en el logro de los objetivos y metas de la Gestión de Seguridad de la información de los usuarios del sistema SAP, cooperando en la mejora continua de las empresas.		
c. En qué medida el nivel del sistema de control interno incide en el grado de aceptación del riesgo de la organización en la Gestión de Seguridad de la información de los usuarios del sistema SAP?	c. Analizar si el nivel del sistema de control interno incide en el grado de aceptación del riesgo de la organización en la Gestión de Seguridad de la información de los usuarios del sistema SAP.	c. El nivel del sistema de control interno inciden adecuadamente en el grado de aceptación del riesgo de la organización en la Gestión de Seguridad de la información de los usuarios del sistema SAP, evaluando los riesgos de las empresas.		
d. En qué medida las acciones de control incide en la efectividad de las operaciones de la Gestión de Seguridad de la información de los usuarios del sistema SAP?	d. Definir las acciones de control incide en la efectividad de las operaciones de la Gestión de Seguridad de la información de los usuarios del sistema SAP.	d. Las acciones de control inciden en la efectividad de las operaciones de la Gestión de Seguridad de la información de los usuarios del sistema SAP, impulsando el cumplimiento de las normas y procedimientos establecidos.		
e. De qué manera el seguimiento de las recomendaciones incide en el grado de eficiencia y eficacia de la Gestión de Seguridad de la información de los usuarios del sistema SAP?	e. Comprobar si el seguimiento de las recomendaciones incide en el grado de eficiencia y eficacia de la Gestión de Seguridad de la información de los usuarios del sistema SAP.	e. El seguimiento de las recomendaciones incide satisfactoriamente en el grado de eficiencia y eficacia de la Gestión de Seguridad de la información de los usuarios del sistema SAP, potenciando los controles en las empresas.		
f. En qué medida los informes de auditoría incide en el fortalecimiento de las políticas y normas de la seguridad de la información de los usuarios del sistema SAP?	f. Demostrar si los informes de auditoría incide en el fortalecimiento de las políticas y normas de la seguridad de la información de los usuarios del sistema SAP.	f. Los informes de auditoría incide razonablemente en el fortalecimiento de las políticas y normas de la seguridad de la información de los usuarios del sistema SAP, mejorando los niveles de gestión en las empresas.		

ANEXO N° 02 – GUIA DE LA ENCUESTA

Instrucciones:

La presente técnica tiene por finalidad recoger información de interés para el estudio, el mismo que está referido a ***"LA AUDITORIA INTERNA Y SU INCIDENCIA EN LA OPTIMIZACIÓN DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACION DE LOS USUARIOS DEL SISTEMA SAP DE LAS EMPRESAS DE SERVICIOS LOGÍSTICOS EN LA PROVINCIA CONSTITUCIONAL DEL CALLAO, AÑO 2016-2017"***. Al respecto, se le pide que en las preguntas que a continuación se acompaña, tenga a bien elegir la alternativa que considere apropiada, marcando para tal fin con un aspa (X) en el espacio correspondiente. Los datos proporcionados serán utilizados con fines académicos. Esta técnica es anónima, se agradece su participación.

1. **En su opinión, ¿está de acuerdo que el Auditor debe tener un grado independencia y objetividad para desarrollar su trabajo en las empresas?**

   a) De acuerdo ( )
   b) Totalmente de acuerdo ( )
   c) Ni acuerdo ni en desacuerdo ( )
   d) En desacuerdo ( )
   e) Totalmente en desacuerdo ( )

   Justifique su respuesta:

   ……
   ……
   ……
   ……..

2. **¿Diga usted, si el valor agregado del trabajo del auditor son las recomendaciones contenidas en la carta de control interno en las empresas?**

   a) De acuerdo ( )
   b) Totalmente de acuerdo ( )
   c) Ni acuerdo ni en desacuerdo ( )
   d) En desacuerdo ( )
   e) Totalmente en desacuerdo ( )

   Justifique su respuesta:

……
……
……
……..

3. **¿En su opinión, el Auditor debe evaluar el nivel de control interno implementado en las empresas?**

a) De acuerdo ( )
b) Totalmente de acuerdo ( )
c) Ni acuerdo ni en desacuerdo ( )
d) En desacuerdo ( )
e) Totalmente en desacuerdo ( )

Justifique su respuesta:

……
……
……
……

4. **¿Considera usted, que las acciones de control contenidas en el Plan Anual de Control se aplican oportunamente por Auditoría Interna?**

a) De acuerdo ( )
b) Totalmente de acuerdo ( )
c) Ni acuerdo ni en desacuerdo ( )
d) En desacuerdo ( )
e) Totalmente en desacuerdo ( )

Justifique su respuesta:

……
……
……
……

5. **¿Cree usted, que el seguimiento de recomendaciones contenidas en el Informe, constituye una herramienta de gestión para la mejora de las empresas?**

a) De acuerdo ( )
b) Totalmente de acuerdo ( )
c) Ni acuerdo ni en desacuerdo ( )
d) En desacuerdo ( )
e) Totalmente en desacuerdo ( )

Justifique su respuesta:

……

……

……

6. **¿Para usted, los Informes de Auditoría Interna contribuyen en el desarrollo de la gestión en las empresas?**

a) De acuerdo ( )
b) Totalmente de acuerdo ( )
c) Ni acuerdo ni en desacuerdo ( )
d) En desacuerdo ( )
e) Totalmente en desacuerdo ( )

Justifique su respuesta:

……

……

……

……

7. **En su opinión, ¿Considera que la función de Auditoría Interna cumple un papel importante en las empresas de servicios logísticos?**

a) De acuerdo ( )
b) Totalmente de acuerdo ( )
c) Ni acuerdo ni en desacuerdo ( )
d) En desacuerdo ( )
e) Totalmente en desacuerdo ( )

Justifique su respuesta:

……

……

……

……

8. **¿Considera Ud., que los planes de seguridad aportan en la prevención de los riesgos en las empresas?**

a) De acuerdo ( )
b) Totalmente de acuerdo ( )
c) Ni acuerdo ni en desacuerdo ( )
d) En desacuerdo ( )
e) Totalmente en desacuerdo ( )

Justifique su respuesta:

……

……

……

……

9. **¿Piensa Ud., que el logro de los objetivos y metas en las empresas de servicios logísticos, es adecuado?**

a) De acuerdo ( )
b) Totalmente de acuerdo ( )
c) Ni acuerdo ni en desacuerdo ( )
d) En desacuerdo ( )
e) Totalmente en desacuerdo ( )

Justifique su respuesta:

……

……

……

……

10. **¿Para usted, está de acuerdo el grado de aceptación del riesgo de la organización es el manejable o administrable?**

a) De acuerdo ( )
b) Totalmente de acuerdo ( )
c) Ni acuerdo ni en desacuerdo ( )
d) En desacuerdo ( )
e) Totalmente en desacuerdo ( )

Justifique su respuesta:

……
……
……
……

11. **¿Para usted, la efectividad de las operaciones son reportadas de manera sustentada en la empresa?**

a) De acuerdo ( )
b) Totalmente de acuerdo ( )
c) Ni acuerdo ni en desacuerdo ( )
d) En desacuerdo ( )
e) Totalmente en desacuerdo ( )

Justifique su respuesta:

……
……
……
……

12. **¿Considera usted, que el grado de eficiencia y eficacia tienen concordancia con los resultados obtenidos por las empresas?**

a) De acuerdo ( )
b) Totalmente de acuerdo ( )
c) Ni acuerdo ni en desacuerdo ( )

d) En desacuerdo ( )
e) Totalmente en desacuerdo ( )

Justifique su respuesta:

……

……

……

13. ¿Cree usted, que las políticas y normas de la seguridad de información, es óptimo en las empresas?

a) De acuerdo ( )
b) Totalmente de acuerdo ( )
c) Ni acuerdo ni en desacuerdo ( )
d) En desacuerdo ( )
e) Totalmente en desacuerdo ( )

Justifique su respuesta:

……

……

……

14. En su opinión ¿La gestión de seguridad de la información es la adecuada en las empresas de servicios logísticos?

a) De acuerdo ( )
b) Totalmente de acuerdo ( )
c) Ni acuerdo ni en desacuerdo ( )
d) En desacuerdo ( )
e) Totalmente en desacuerdo ( )

Justifique su respuesta:

……

……

……

……

ANEXO N° 03

APORTES DEL INVESTIGADOR PARA LOS AUDITORES INTERNOS Y LAS EMPRESAS LOGISTICAS

A) AUDITORES INTERNOS:

La presente investigación tiene como propósito dar a conocer las pautas a seguir por los Auditores Internos en la revisión de los Perfiles de usuarios en el sistema SAP, detallamos:

1. Revisar detalladamente los informes de la Auditoría de TI, Auditoría Interna y Externa acerca de las deficiencias de control y riesgos de tecnología existente en la empresa.

2. Identificar y realizar el seguimiento de las observaciones de los informes anteriores que a la fecha no hayan sido subsanadas (validaciones en el sistema SAP).

3. Verificación y difusión del cumplimiento de Políticas de Gestión de usuarios y Control de Accesos SAP, Políticas de Seguridad de Información.

4. Verificación del cumplimiento de los Estándares de Nomenclatura de usuarios, Roles SAP y Administración de Cuentas y Accesos SAP.

5. Revisión y validación de la Matriz de actividades y transacciones por cada módulo SAP (Finanzas, Compras, Ventas, Controlling, Recursos Humanos, Calidad, Producción, etc.), detallando la descripción de cada actividad (concepto, propósito, utilidad), con la finalidad de clasificar por nivel de criticidad y sustentar su criticidad (posibilidad del riesgo).

6. Identificar aquellos usuarios que concentren dos o más responsabilidades en un mismo proceso que generen conflicto de segregación de funciones; asimismo, revisar la estadística de uso de los accesos otorgados, a fin de validar su utilización o recomendar su retiro en su perfil de usuario.

7. Validar y definir las reglas de segregación para los procesos de las empresas del Grupo Romero, con la finalidad de identificar y evitar que una misma persona concentre dos o más responsabilidades dentro del sistema, de tal forma que pueda realizar acciones o transacciones que lleven a errores operativos y/o fraude.

8. Revisar detalladamente los perfiles de los usuarios identificados, estableciendo sus importes de liberación de compras, aprobación de anticipos de proveedores y personal, acceso a información confidencial, movimientos de almacén, etc.

9. Validar con los Autorizadores de Accesos SAP de la empresa (dueños del proceso) y solicitar la documentación sustentatoria de las aprobaciones a los accesos críticos del personal.

10. Elaborar Flujogramas de los Procesos de la empresa a fin de comprobar con los Autorizadores, se encuentre actualizado de acuerdo a las actividades soportadas por SAP.

11. Verificar que los usuarios genéricos no tengan asignados dentro de sus roles actividades o transacciones críticas que afecte a los procesos del negocio y que se encuentren asignado a un responsable del área.

12. Revisar el reporte de usuarios logueados en el sistema SAP, a fin de identificar el tiempo de duración de las sesiones de los usuarios a la vez en distintos equipos a los asignados.

13. Verificar las vigencias de uso en los perfiles de aquellos usuarios que reemplazan temporalmente a un trabajador (vacaciones, ausencias, permisos, etc.).

14. Revisar que los usuarios inactivos por más 60 días se encuentren bloqueados y por más de 90 días sean eliminados; asimismo, validar las comunicaciones oportunas del área de Recursos Humanos sobre la baja del personal y sus usuarios SAP.

15. Revisión de los formatos de Aceptación de Riesgos firmados por la Dirección y Gerencias correspondientes, en los casos donde se identifique los conflictos de segregación y se establezcan las acciones de control que mitiguen los riesgos asumidos.

16. Seleccionar una muestra de los "Compromiso del Cumplimiento de Políticas de usuarios y Accesos SAP" firmados por los trabajadores de la empresa, el cual debe de adjuntarse a su file que es custodiado en Recursos Humanos.

17. Revisar los acuerdos contractuales de confidencialidad por la asignación de un usuario SAP al personal externo de la empresa (consultores externos, trabajadores temporales y proveedores).

18. Revisar la información del listado de las personas autorizadas que acceden al Data Center, capacitación al personal de seguridad (vigilancia), Verificación de los procedimientos a brindar acceso a personas ajenas a la organización.

19. Analizar la pérdida de valor que se podría originar en caso de ser violentada la seguridad de acceso al Data Center y solicitar planes de contingencias frente a posibles siniestros.

20. Resumir el aporte que se ha logrado para la empresa nuestra auditoría practicada, de preferencia cuantificar este hecho.

B) EMPRESAS LOGÍSTICAS:

La presente investigación tiene como propósito dar a conocer las pautas a seguir en las empresas que brindan servicios logísticos para la gestión y control de los Perfiles de usuarios en el sistema SAP, detallamos:

1. Establecer políticas, procedimientos y estándares formalmente que permitan mantener un control adecuado de los usuarios y accesos durante los cambios generados por los negocios de la empresa.

2. Establecer Comités de seguridad de la información de los perfiles de usuarios SAP, con el objetivo de identificar los principales problemas y formular un modelo de autorizaciones que permita la administración y control de los accesos de manera óptima.

3. Contar con herramientas que soporten el proceso de asignación de accesos a los usuarios tales como: maestros de usuarios actualizado con información de RRHH, un maestro de transacciones organizado y clasificado por procesos de negocios y niveles de criticidad, un sistema de reportes de usuarios, accesos, registros de auditoría, estadísticas de uso, entre otros.

4. Desarrollo de Mapas o Flujogramas de Negocio a nivel de aplicación que nos permita tener un entendimiento común de los procesos de negocio soportados en el sistema SAP.

5. Contar con repositorio digital donde se registren las incidencias o debilidades de control que se originen en la utilización del sistema SAP y que estas sean subsanadas de forma oportuna.

6. Promover programas de capacitación en seguridad de la información para el personal de la empresa.

7. Reducir los riesgos de seguridad basando en un modelo de autorizaciones en el uso del sistema SAP, a fin de contar una efectiva y eficiente administración de las autorizaciones en el sistema SAP.

8. Los autorizadores serán responsables de revisar y aprobar al menos dos veces al año los accesos otorgados al personal a su cargo. Para el cumplimiento de estas políticas el Área de Seguridad de la Información convocará periódicamente los autorizadores para la revisión de accesos.

9. Asignar responsables de validar el modelo de autorizaciones (transacciones, grupos, actividades y mapas de procesos) y proponer cambios.

10. Controlar que los accesos al sistema SAP sean asignados y actualizados de acuerdo a las funciones y responsabilidades de los empleados, de acuerdo a la información del Área de Recursos Humanos.

11. Enlazar el usuario SAP con el código del Colaborador, siendo imprescindible para crear un usuario que el Colaborador se encuentre registrado como empleado en el Modulo SAP de Recursos Humanos.

12. El área Recursos Humanos deberá comunicar al área de Sistemas cuando un Colaborador es dado de baja, con el fin de que se Bloquee/Elimine/Renombre el Usuario asignado al dicho Colaborador.

13. Incorporar como una buena práctica que el Colaborador con un Usuario SAP deberá firmar el “Compromiso de Cumplimiento de Políticas de usuarios y Accesos SAP”, el cual será anexado a su file personal en Recurso Humanos.

14. Los usuarios genéricos podrán ser solicitados únicamente para uso compartido por turnos y las actividades que necesita realizar sobre el sistema son No Críticas, para la creación de un Usuario de este tipo es necesario la aprobación del respectivo Autorizador por Jerarquía.

15. Los accesos de empresas externas deberán contar con un contrato firmado que incluya cláusulas de confidencialidad que impliquen una penalidad económica y legal por incumplimiento.

16. Establecer que los usuarios SAP que se encuentren inactivos por más de 60 días serán bloqueados y los usuarios SAP inactivos por más de 90 días serán eliminados, y se informará de la acción a los Autorizadores por Jerarquía.

17. Proponer y definir reglas de segregación para los procesos de la empresa, con la finalidad de identificar y evitar que una misma persona concentre dos o más responsabilidades dentro del sistema, de tal forma que pueda realizar acciones o transacciones que lleven a errores operativos y/o fraude.

18. Las claves de acceso al sistema SAP deben tener la siguiente complejidad mínima: contener por lo menos una letra mayúscula, una letra minúscula y un número. Las claves de acceso deberán ser cambiadas cada sesenta (60) días.

19. Establecer políticas sobre el adecuado control, inventario y custodia de los activos de información de la empresa.

20. Establecer en el Reglamento Interno de Trabajo que cada Usuario SAP deberá estar asignado exclusivamente a un Colaborador, quien será el responsable de su utilización y de las actividades que se ejecuten en el sistema SAP, considerando como falta grave el compartir su contraseña.