UNIVERSIDAD PRIVADA DEL NORTE

ESCUELA DE POSGRADO

LA AUDITORIA INFORMÁTICA Y LA SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE SISTEMAS DE LA CAJA DEL SANTA, CHIMBOTE - 2018

Tesis para optar el grado **MAESTRO** en:

Ingeniería de Sistemas con Mención en Gerencia de Sistemas de Información

Autores:

Br. Rudy Díaz Limay

Asesor:

Mg. Lomparte Alvarado, Rómulo

Trujillo – Perú

2018

Resumen

El presente trabajo de investigación titulado La auditoría informática y la seguridad de la información en el área de sistemas de la caja del Santa, Chimbote - 2018, tiene como objetivo determinar en qué medida la auditoría informática se relaciona con la seguridad de la información en el área de sistemas de la Caja del Santa; la investigación es de tipo descriptivo correlacional y utiliza un diseño no experimental. La población muestral estuvo conformada por 10 trabajadores de la institución objeto de estudio; se utilizó como técnica de recolección de datos la encuesta y como instrumento derivado de ello el cuestionario (Anexo 1); posterior a la aplicación de los instrumentos, se procesaron los datos en el software estadístico SPSS, obteniéndose una correlación R de Pearson moderada de 0.640, significativa al 1% (0.009), por lo tanto, con los resultados obtenidos, se acepta la hipótesis que establece que la auditoría informática se relaciona significativamente con la seguridad de la información en el área de sistemas de la Caja del Santa, Chimbote 2018.

Abstract

This research work entitled Impact of computer audit and information security in the systems area of the Santa, Chimbote - 2018 box, aims to determine to what extent the information audit relates to information security in the systems area of the Caja del Santa; the research is descriptive correlational and uses a non-experimental design. The sample population consisted of 10 workers from the institution under study; the survey was used as a data collection technique and the questionnaire as a derived instrument; after the application of the instruments, the data were processed in the statistical software SPSS, obtaining a moderate Pearson R correlation of 0.640, significant at 1% (0.009), therefore, with the results obtained, the hypothesis that establishes that the computer audit is significantly related to information security in the systems area of the Caja del Santa, Chimbote 2018

Dedicatoria y agradecimiento

A mi creador Jehová, a mi esposa Karin, a mi hija Mía, a mis padres Víctor y María, a mis hermanos Víctor y Miluska, sobrinos y Familia en general, puesto que ellos son las personas más importantes en mi vida, personas que siempre están presentes para dedicarme parte de su tiempo, para apoyarme incondicionalmente en cada decisión que considero que es la correcta, alentarme a seguir adelante, dándome apoyo moral; aconsejándome para el desarrollo de mi vida personal y profesional.

Rudy Weslie Díaz Limay

Tabla de contenidos

Índice de tablas

Índice de figuras

I. INTRODUCCIÓN

1.1. Realidad problemática

El avance tecnológico de los sistemas y telecomunicaciones han alcanzado gran evolución, junto con eso en la misma proporción avanzan los riesgos asociados a las mismas, y hoy en día para muchas empresas del Perú, sean privadas o públicas, la seguridad de la información es un problema que poseen en común, debido a que pocas de estas empresas plantean medidas de contingencia para salvaguardar el activo más importante hoy considerado como lo es La Información.

A nivel nacional, se tiene el caso de la empresa Card Perú S.A, entidad emisora de tarjetas de crédito, la probabilidad de que la información sea interceptada, robada y modificada por personas inescrupulosas y sin autorización de acceso a esta es un latente; de igual forma sucedió con el Banco BCP, el cual fue vulnerado su sistema de seguridad informática atreves de un dispositivo USB, el cual permitió el retiro de dinero de las cuentas de los clientes.

Estos hechos resultan peligrosos para la organización, ya que mucha de la información fundamental e importante para la realización de procesos críticos del negocio puede ser vulnerada y amenazada ocasionando la interrupción de estos procesos; que conllevan de esta manera, a una pérdida no solo de información, sino también financiera.

La mencionada problemática detallada líneas atrás, se presenta en el área de sistemas de la Caja del Santa, en la misma se despliega una lista de eventualidades relacionadas al tema de la seguridad de la información, ello se grafica en la carencia de procedimientos de seguridad tales como, la falta de respaldo de información o copia de respaldo, no existen control o permisos definidos a la información confidencial de la empresa, lo que generaría que se vulnere la integridad de los datos no solo del área objeto de estudio, si no, de todas las áreas a la que se tiene acceso, así también se evidencia que de ser el caso que se desea solicitar información específica, la misma no se encuentra disponible en el acto; en conjunto las medidas preventivas para resguardar la información de la empresa no se

encuentran implementadas; un dato o caso problemático que se ha suscitado producto la falta de una auditoría informática y seguridad de la información fue la pérdida del historial de clientes durante los meses de enero a julio del 2017, lo que generó en un primer punto la desafiliación de aquellos clientes, ocasionando fuertes pérdidas económicas para la empresa, además de una mala imagen para la misma.

Por lo tanto, es de necesidad determinar como la auditoría informática se relaciona con la seguridad de la información en el área de sistemas de la Caja del Santa.

1.2. Pregunta de investigación

¿En qué medida la auditoría informática se relaciona con la seguridad de la información en la Caja del Santa?

1.3. Objetivos de la investigación

Objetivo General

- Determinar en qué medida la auditoría informática se relaciona con la seguridad de la información en la Caja del Santa.

Objetivos Específicos

- Identificar el nivel actual de los procedimientos contemplados en la auditoría informática aplicados en el área de sistemas de la Caja del Santa
- Diagnosticar el nivel de seguridad de la información en el área de sistemas de la Caja del Santa
- Identificar e interpretar la correlación entre la auditoría informática y la seguridad de la información mediante el coeficiente R de Pearson en el área de sistemas de la Caja del Santa.

1.4. Justificación de la investigación

La investigación se justifica por el aporte que brindará la investigación sobre como la auditoría informática se relaciona con la seguridad de la información en la empresa del rubro bancario cómo la Caja del Santa, sirviendo como base teórica para futuras investigaciones que deseen conocer la causalidad de las variables que son objeto de estudio. Los resultados obtenidos producto

de las investigaciones realizadas, al mismo tiempo de la importancia del análisis de estos resultados, generará una solución lógica referido a la seguridad de la información de las empresas o instituciones, dado que en la actualidad aún no se ha realizado estudios referidos al tema en la institución objeto de estudio.

Así mismo el presente proyecto de investigación dará lugar a nuevas bases teóricas, además de que los resultados arrojados producto de la investigación servirán para investigaciones futuras sobre el tema tratad, al mismo tiempo la presente investigación generará nuevas estrategias en cuanto a la seguridad de la información y su relación con la auditoría informática, que pueden optar las empresas del rubro bancario. Entre tanto aporta información que permitirá evidenciar la causalidad de las variables, donde las mismas sirven de referencia para posteriores investigaciones en este ámbito, tanto en el plano local, regional y nacional.

1.5. Alcance de la investigación

En la presente investigación se va a determinar en qué medida la auditoría informática se relaciona con la seguridad de la información, colaborando con la reducción de la probabilidad o impacto de los riesgos que puedan afectar a los distintos procesos de los sistemas en estudio, es decir permitirá conocer en el futuro los riesgos asociados a las tecnologías de la información para que mediante la aplicación de normas, estándares y mejores prácticas los riesgos sean conocidos, gestionados y controlados, y de esa forma salvaguardar y manejar adecuadamente la información que día a día se ingresa aplicando una guía debidamente estructurada como lo es la propuesta del plan de auditoria informática.

II. MARCO TEÓRICO

2.1. Antecedentes

A nivel internacional se tiene la investigación de Jara (2013) en su tesis denominada “Auditoría informática de la gestión de ti para la empresa “Advance Consulting” utilizando el modelo COBIT.”, con el principal objetivo de duplicar la cantidad de clientes que se tiene actualmente e incrementar su personal e incrementar su infraestructura, a nivel de oficina, hardware y

software, para ello la investigación estuvo bajo el diseño pre-experimental, luego del procesamiento de los datos, se llegó a la conclusión que mediante el modelo COBIT, se ha podido evaluar y diagnosticar los procesos de TI en la Empresa “Advance Consulting”, de manera que se pudo identificar riesgos, gestionar recursos y medir el desempeño, así como el nivel de madurez de cada uno de los procesos de la empresa objeto de estudio; así también, con el adecuado manejo de una gestión de TI se pudo identificar que todo el personal cumple funciones importantes necesarias y complementarias en el Área Informática.

Así también se tiene la investigación de Coronel (2013), en su tesis titulada “Auditoria informática orientada a los procesos críticos de créditos generados en la Cooperativa Ahorro y Crédito Fortuna aplicando el marco de trabajo COBIT”, la cual tuvo como objetivo principal el desarrollo del proceso de una auditoría informática para evaluar y determinar el nivel de cumplimiento de los procesos críticos de crédito de la empresa objeto de estudio, teniendo como metodología de trabajo a COBIT, para ello se aplicó la metodología de los modelos de madurez del COBIT; finalmente se se planteó un plan de acción el cual pretende facilitar la toma de decisiones por parte de los directivos de la institución. Se llegó a la conclusión que se conocieron los procedimientos crediticios internos de la cooperativa, pudiéndose determinar que los procesos de crédito son realizados en un 40% mediante un sistema automatizado y el 60% de estos procesos de crédito son realizados de forma manual, lo que supone un coste alto, tanto en recursos como en tiempo de trabajo para las oficiales de crédito de la institución.

A nivel local, se tiene la investigación de Ramos (2015), en su tesis titulada Propuesta de un plan de auditoria informatica para el sistema de informacion en salud y el aplicativo para el registro de formatos sis" en los establecimientos de salud de la unidad ejecutora 400 en la region Piura, con el principal objetivo de proponer un plan de auditoría informática en los establecimientos de salud de la Unidad Ejecutora 400 en la Región Piura

para el Sistema de Información en Salud y el Aplicativo para el Registro de Formatos SIS, llegándose a la conclusión que en base al marco normativo peruano se desarrolló la propuesta del plan de auditoría informática que permite obtener una guía para las futuras auditorías a los sistemas informáticos del estado peruano (Aplicativo para el Registro de Formatos SIS y al Sistema de Información en Salud). (estado del arte)

2.2. Auditoría Informática

2.2.1. Teorías de auditoría informática

Auditoria

Proceso para determinar el cumplimiento con los requerimientos, planes y contrato, según aplique. Se indica además que este proceso puede ser empleado por cualesquiera de las dos partes, donde una de ellas (la auditora) audita los productos software o actividades de la otra parte (la auditada).

Según ISACA, la auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes. (Ramos, 2015)

Tipos de Auditorias

Una de las clasificaciones que se propone es:

Auditorias por su lugar de aplicación

Auditoría externa

Auditoría interna

Auditorias por su área de aplicación

Auditoría financiera

Auditoría administrativa

Auditoría operacional

Auditoría integral

Auditoría gubernamental

Auditoría de sistemas

Auditorias especializadas en áreas especificas

Auditoría al área médica (evaluación médico sanitaria)

Auditoría al desarrollo de obras y construcciones (evaluación de ingeniería)

Auditoría fiscal

Auditoría laboral

Auditoría de proyectos de inversión

Auditoría a la caja chica o caja mayor (arqueos)

Auditoría al manejo de mercancías (inventarios)

Auditoría ambiental

Auditoría de sistemas

Auditoría de sistemas computacionales

Auditoría informática

Auditoría con la computadora

Auditoría sin la computadora

Auditoría a la gestión informática

Auditoría al sistema de cómputo

Auditoría alrededor de la computadora

Auditoría de la seguridad de sistemas computacionales

Auditoría a los sistemas de redes

Auditoría integral a los centros de cómputo

Auditoría IS0-9000 a los sistemas computacionales

Auditoría outsourcing

Auditoría ergonómica de sistemas computacionales

(Ramos, 2015)

Auditoría Informática

Uno de los conceptos encontrados es:

Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la

gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo. El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa. (Ramos, 2015)

COBIT

COBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información (TI) – COBIT es la herramienta innovadora para el gobierno de TI (Governance. Término aplicado para definir un control total).

COBIT se fundamenta en los Objetivos de Control existentes de la Information Systems Audit and Control Foundation (ISACF), mejorados a partir de estándares intencionales técnicos, profesionales, regulatorios y específicos para la industria, tanto existentes como en surgimiento. Los Objetivos de control resultantes han sido desarrollados para su aplicación en sistemas de información en toda la empresa. El término “generalmente aplicable y aceptado” es utilizado explícitamente en el mismo sentido que los Principios de Contabilidad Generalmente aceptados. Para propósitos del proyecto, “buenas prácticas” significa consenso por parte de los expertos.

Este estándar es relativamente pequeño en tamaño, con el fin de ser práctico y responder, en la medida de lo posible, a las necesidades de negocio, manteniendo al mismo tiempo una independencia con respecto a las plataformas técnicas de TI adoptadas en una organización. El proporcionar indicadores de desempeño (normas, reglas, etc.), ha sido

identificado como prioridad para las mejoras futuras que se realizarán en el marco referencial. (Nazareno, 2016)

En muchas ocasiones se relaciona a la auditoría como una rendición de cuentas en donde el fin último sería detectar errores, sin embargo, el concepto de auditoría va más allá de eso, es un procedimiento periódico, que debe realizarse con el objeto de evaluar la eficacia y eficiencia de una institución o de parte de ella. Hernández sostiene que la auditoría es un proceso necesario para las organizaciones con el fin de asegurar que todos sus activos sean protegidos en forma adecuada. En donde, la alta dirección espera que de estos procesos de auditoría surjan recomendaciones necesarias para la mejora continua de las funciones de la organización. (Hernández, citado en Carrizo, 2013).

Existen otros autores como Kell y Ziegler que orientan el concepto de auditoría a la obtención de resultados que deberán ser comunicados a la parte interesada, los mismos definen a la auditoría como un proceso para obtener y evaluar evidencias. (Ziegler, s.f).

Los conceptos anteriores hacen referencia a la auditoría de manera general, de los cuales se derivan las definiciones actuales de auditoría informática. Por lo tanto, se orienta a la verificación y aseguramiento de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología de la información en la organización, se lleven a cabo de una manera oportuna y eficiente. (Del Peso, citado en Vanegas, 2016).

La auditoría informática es un proceso necesario que debe ser realizado por personal especializado para garantizar que todos los recursos tecnológicos operen en un ambiente de seguridad y control eficientes, de manera que la entidad tenga la seguridad de que opera con información verídica, integral, exacta y confiable. Además, la auditoría deberá contener observaciones y recomendaciones para el mejoramiento continuo de la tecnología de la información en la institución.

2.2.2. Objetivos de la Auditoría Informática

Del Peso, citado en Vanegas (2016), sostiene que la auditoria informática confirma la consecución de los objetivos tradicionales de la auditoria: objetivos de protección de activos e integridad de datos; y objetivos de gestión, que abarcan no solamente los de protección de activos, sino también los de eficacia y eficiencia.

2.2.3. Bases de la Auditoría Informática

Simón, citado en Vanegas (2016), en su obra Auditoría Informática, considera a la Auditoría Informática (AI) como la intersección de cuatro disciplinas: Auditoría Tradicional, Ciencias del Comportamiento, Gestión de Sistemas de Información e Informática.

2.2.4. Funciones de la Auditoría Informática

Dentro del proceso de auditoría es importante asegurar que se cumplan por lo menos los principios básicos de un proceso formal. Los elementos indispensables para cumplir este requisito son: la planeación, el control y el seguimiento del desempeño, que deberán garantizar lo siguiente: (Apuntes de Auditoría Informática, citado en Vanegas, 2016).

- Que los recursos de informática sean orientados al logro de los objetivos y las estrategias de las organizaciones.
- La elaboración, difusión y cumplimiento de las políticas, controles y procedimientos inherentes a la AI.
- Que se den los resultados esperados por la institución mediante la coordinación y apoyo reciproco con: auditoría, asesores externos, informática, y la alta dirección.

2.2.5. Importancia del Control y la Auditoría Informática

Simón, citado en Vanegas (2016), en sus apuntes de Auditoría Informática hace referencia a algunos factores críticos que atentan al bien más preciado de una organización en la actualidad, la información. Estos factores son: coste de la pérdida de datos, toma de decisiones incorrecta, abuso informático, y privacidad de los datos.

2.2.6. Metodología de desarrollo de la Auditoría Informática

Kuna, citado en Álvarez (2015) en su Tesis de Magister: "Asistente para la realización de Autoría de Sistemas en Organismos Públicos o Privados", enuncia una metodología de desarrollo de AI muy general, que coincide con varias propuestas de diferentes autores. Se contemplan las siguientes fases:

Fase 1. Identificar el alcance y los objetivos de la Auditoría Informática

En esta fase se determinan los límites y el entorno en que se realizará la auditoría, debe existir un acuerdo muy preciso entre autoridades y auditores. El éxito del proceso depende de una clara definición de esta etapa. (Kuna, citado en Álvarez, 2016).

Fase 2. Realizar el estudio inicial del entorno a auditar

En esta fase es necesario examinar las funciones y actividades generales de la organización a auditar y en particular de las relacionadas con las tecnologías de la información. Se debe definir el organigrama, los departamentos, las relaciones funcionales y jerárquicas entre las distintas áreas de la organización, el flujo de información, el número de puestos de trabajo y personas por puesto de trabajo, la estructura organizativa del departamento de informática, características de hardware y software, las metodologías de desarrollo y mantenimiento de aplicaciones, y aspectos relacionados con la seguridad. (Kuna, 2006).

Fase 3. Determinación de los recursos necesarios para realizar la auditoría informática

Después de realizar el estudio preliminar se debe determinar los recursos materiales y humanos necesarios para implementar el plan de auditoría. (Kuna, citado en Álvarez, 2016).

Fase 4. Elaborar el plan de trabajo

En esta fase se define el calendario de actividades a realizar, formalizando el mismo para la aprobación por parte de las autoridades. (Kuna, citado en Álvarez, 2016).

Fase 5. Realizar las actividades de auditoría

Es el momento donde se efectivizan las actividades planificadas en la fase anterior, aplicando distintas técnicas y utilizando herramientas que garanticen el cumplimiento de los objetivos planteados. (Kuna, citado en Álvarez, 2016).

Fase 6. Realizar el informe final

"La elaboración del Informe Final es la única referencia constatable de toda auditoría, y el exponente de su calidad." (Kuna, citado en Álvarez, 2016, p. 25).

Kuna presenta un modelo estándar de la estructura del informe final para cada proceso evaluado, en el cual intervienen: definición de objetivos, situación actual, tendencias, puntos débiles, amenazas y recomendaciones. (Kuna, citado en Álvarez, 2016).

Fase 7. Carta de Presentación

Es la última etapa de la auditoría consta de un resumen del contenido del informe final, dirigido a las autoridades de la institución. (Kuna, citado en Álvarez, 2016).

a. Estudio de la normativa existente para auditorías informáticas

- **Normas, Técnicas, Estándares y Procedimientos de Auditoría**

  Actualmente el desarrollo de una auditoría informática se basa en la aplicación de normas, técnicas, estándares y procedimientos que garanticen el éxito del proceso. La gran mayoría de documentación existente coincide en que las normas de auditoría son requisitos mínimos de calidad, relativos a las cualidades del auditor, a los

métodos y procedimientos aplicados en la auditoría, y a los resultados. (Aguirre, s.f).

Las técnicas en cambio, son todos aquellos métodos que permiten al auditor evidenciar y fundamentar sus opiniones y conclusiones. (Secretaría de la Función Pública – México, citado en Álvarez, 2016).

- **Organizaciones y Normas de AI más relevantes**

Actualmente el Ecuador cuenta con un marco regulatorio y normativo reducido en materia informática, es por ello que se estudiarán las normas y organizaciones internacionales más relevantes en este ámbito. Las organizaciones más importantes son: Institute of Internal Auditors (IIA), e Information System Audit and Control Association (ISACA)

Las organizaciones antes mencionadas, han desarrollado normas y estándares con el fin de establecer políticas y lineamientos que garanticen el proceso de auditoría. Algunos de los estándares más conocidos son:

- **COBIT:** Control Objectives for Information and related Technology.

  Desarrollado por Information Systems Audit and Control Association (ISACA). Centra su interés en la gobernabilidad, aseguramiento, control y auditoría para Tecnologías de la Información y Comunicación (TIC).

- **ITIL:** Information Technology Infrastructure Library.

  Recoge las mejores prácticas para administrar los servicios de Tecnología de la Información (TI).

- **COSO:** Committee of Sponsoring Organizations.

  Hace recomendaciones a los administradores de TI sobre cómo evaluar, informar e implementar sistemas de control, teniendo como objetivo la efectividad y eficiencia de las operaciones, la información financiera y el cumplimiento de las regulaciones, valoración de

riesgos, actividades de control, información y comunicación y la verificación.

- **ISO Serie 27000**

  Integra un conjunto de normas sobre Sistemas de Gestión de Seguridad de la Información (SGSI), que, a través de su aplicación, permite administrar la información mediante el modelo Plan – Do – Check – Act(PDCA).

2.3. Seguridad de la información

Un sistema de seguridad de información es un conjunto de responsabilidades, procesos, procedimientos y recursos que establece la alta dirección con el propósito de dirigir y controlar la seguridad de los activos de información y asegurar la continuidad de la operatividad de la empresa. (Álvarez, 2016)

2.3.1. Definición

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicas que permitan resguardan y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

La información puede ser clasificada de la siguiente manera:

- **Crítica:** Es indispensable para la operación de la empresa
- **Valiosa:** Es un activo de la empresa y muy valioso

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y se debe sabe que puede ser confidencial. Puede ser divulgada, mal utilizada, robada, borrada, saboteada, etc. (Álvarez, 2016)

2.3.2. Definición de riesgo

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema.

Entre las amenazas, existen las vulnerabilidades, los riesgos y los activos de información, una secuencia de causalidad y probabilidad de ocurrencia.

III. HIPÓTESIS

La auditoría informática se relaciona positivamente en la seguridad de la información en la Caja del Santa.

IV. DECLARACIÓN DE HIPÓTESIS

Variable independiente:

Auditoría informática

Variable dependiente:

Seguridad de la información

V. OPERACIONALIZACIÓN DE VARIABLES

Variable	Tipo de Variable	Operacionalización	Categorías o Dimensiones	Definición	Indicador	Nivel de Medición
AUDITORIA INFORMÁTICA	CUALITATIVA	Proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo empresarial, mantiene la integridad de los datos ya que esta lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, cumple con las leyes y regulaciones establecidas	PRELIMINAR	DIAGNÓSTICO DEL ESTADO ACTUAL DE LA PARTE INFORMÁTICA	DIAGNOSTICO DE NEGOCIO	INTERVALO
					DIAGNOSTICO DE INFORMÁTICA	
			JUSTIFICACIÓN	ES DONDE SE JUSTIFICA LA REVISIÓN O EVALUACIÓN DE LAS AREAS O FUNCIONES CRITICAS RELACIONADAS CON INFORMATICA	MATRIZ DE RIESGOS/JUSTIFICACIÓN POR AREA DE REVISION	
					PLAN GENERAL DEL PROYECTO DE AUDITORIA INFORMÁTICA	
			ADECUACIÓN	SE ENFOCA EN EL ANÁLISIS, ADECUACIÓN Y ACTUALIZACIÓN DE TODOS LOS ELEMENTOS QUE SE INVOLUCRAN EN UN PROYECTO DE AUDITORIA DE INFORMÁTICA	PLAN DE AUDITORIA INFORMATICA	
					ASPECTOS A EVALUAR	
					TECNICAS Y HERRAMIENTAS	
					POLITICAS Y PROCEDIMIENTOS	
			FORMALIZACIÓN	SE BUSCA LA APROBACIÓN Y APOYO FORMAL PARA EL DESARROLLO DEL PROYECTO DE AUDITORÍA DE INFORMÁTICA PRESENTADO POR EL LIDER DEL PROYECTO	VERIFICACIÓN DE PRIORIDADES	
			DESARROLLO	ES LA MAS IMPORTANTE PARA EL AUDITOR DE	PRESENTACIÓN FORMAL DEL PLAN DE AUDITORÍA	

				INFORMÁTICA, YA QUE ES AQUÍ DONDE SE EJERCE SU FUNCIÓN DE MANERA PRÁCTICA, EMPEZANDO A EJECUTAR LAS TAREAS DE SU TRABAJO DE ACUERDO AL PLAN APROBADO	CRONOGRAMA DE ENTREVISTAS, APLICACIÓN DE CUESTIONARIOS Y VISITAS	
					CLASIFICACION DE TECNICAS, HERRAMIENTAS, CUESTIONARIOS Y ENTREVISTAS	
					APLICACIÓN DE ENTREVISTAS	
					INFORME PRELIMINAR	
					ELABORACIÓN Y PRESENTACIÓN FINAL DEL INFORME	
SEGURIDAD DE LA INFORMACIÓN	CUALITATIVA	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	CONFIABILIDAD	LA PROBABILIDAD QUE LA INFORMACIÓN ESTÉ DISPONIBLE Y NO SEA DIVULGADA A PERSONAS NO AUTORIZADAS	PROBABILIDAD DE DISPONIBILIDAD DE INFORME	NOMINAL
			INTEGRIDAD	PROPIEDAD DE SALVAGUARDAR LA EXACTITUD E INTEGRIDAD DE LOS ACTIVOS	NIVEL DE INTEGRIDAD DE LOS ARCHIVOS	
			DISPONIBILIAD	LA PROPIEDAD DEBE ESTAR DISPONIBLE Y UTILIZABLE CUANDO SE REQUIERA	NIVEL DE DISPONIBILIDAD DE ARCHIVOS A PERSONAS AUTORIZADAS	

VI. DESCRIPCIÓN DE MÉTODOS Y ANÁLISIS

6.1. Universo

Los universos de personas estuvieron integrados por profesionales de la carrera de informática que participaron en los procesos de auditoria llevados a cabo en la empresa objeto de estudio, los mismos representan el 100% de la población. (Véase Anexo N° 03: Ficha Técnica del Universo)

6.2. Población

La población del presente trabajo de investigación estuvo constituida por 10 trabajadores del área de sistemas de la Caja del Santa del Distrito de Nuevo Chimbote, tal como se muestra a continuación.

Área de sistemas	Total de trabajadores
Trabajadores	10
Total	10

Fuente: Caja del Santa

6.3. Muestra

Para el caso de la investigación la muestra tuvo la misma cantidad de la población.

6.4. Técnica

Encuesta:

Sirvió para la obtención de datos de la población de estudio, con el fin de conocer estados de opinión o hechos específicos.

6.5. Instrumentos

Cuestionario:

Se utilizó para la obtención información de la población de estudio por medio de una serie de enunciados representados por una escala de pesos (escala de Likert). (Anexo N° 01 y 02)

El presente cuestionario estuvo clasificado en base a los indicadores de las variables objeto de estudio; para el caso de determinar el nivel de seguridad de información, estuvo medida en base a la escala de Likert.

6.6. Análisis y procesamiento de información

Para el análisis y procesamiento de información recopilada mediante la aplicación de los instrumentos, se empleó los cuadros de frecuencia y porcentajes, así como los gráficos de barras. El estadístico inferencial empleado fue la correlación R de Pearson.

Posterior al procesamiento de datos y obtenido los puntajes promedio para cada variable, se procedió a determinar en qué nivel se encuentran los mismos.

VII. RESULTADOS

A continuación, se presentan los resultados producto de la aplicación del cuestionario a la población objeto de estudio, los mismos se concretizan según los objetivos especificados, dichos resultados son presentados en tablas de frecuencia y gráficos de barras; el procesamiento de la información se realizó en el software estadístico SPSS Y EXCEL.

VARIABLE AUDITORÍA INFORMÁTICA

A continuación, se presenta los niveles de las dimensiones de la auditoría informática:

Tabla 1. Niveles de las dimensiones de la auditoría informática

	DIMENSIONES DE LA AUDITORIA INFORMÁTICA				
NIVELES	**PRELIMINAR**	**JUSTIFICACIÓN**	**ADECUACIÓN**	**FORMALIZACIÓN**	**DESARROLLO**
Ineficiente	70.00%	80.00%	40.00%	70.00%	60.00%
Inicio	20.00%	10.00%	30.00%	20.00%	20.00%
Medianamente satisfactorio	10.00%	10.00%	30.00%	10.00%	20.00%
Eficiente y satisfactorio	0.00%	0.00%	0.00%	0.00%	0.00%

Fuente: Instrumento aplicado (Anexo 1)

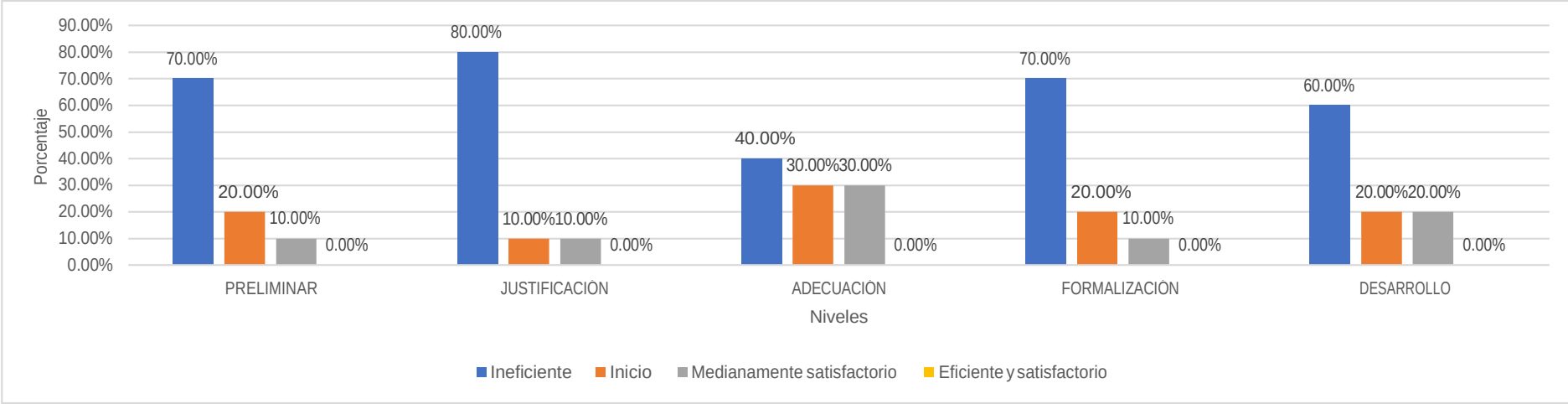


Figura 1: Niveles de las dimensiones de la auditoría informática

Fuente: Tabla 1 (Véase Anexo N° 03: Ficha Técnica del Universo)

En la Tabla y Figura 1 se observa respecto a las dimensiones de la auditoría informática, en cuanto a la dimensión preliminar, la misma se encuentra en un nivel ineficiente, validado por el 70% de la población encuestada, que representan 7 trabajadores del área de sistemas, mientras tanto solo el 10%, que representan a 1 trabajador, manifiesta que se encuentra en un nivel medianamente satisfactorio. Por otro lado, para el caso de la dimensión justificación, se denota que más de la mitad, es decir el 80% de la población encuestada, manifiesta que la mencionada dimensión se encuentra en un nivel ineficiente y solo el 10% aduce que se encuentra en niveles de inicio y medianamente satisfactorio respectivamente.

En cuanto a la dimensión adecuación, el 40% de la población manifiesta que se encuentra en un nivel de inicio, mientras tanto el 30% y 30% respectivamente la califican en niveles de inicio y medianamente satisfactorio. Respecto a la dimensión formalización, se evidencia que se encuentra en un nivel ineficiente en un 70% (manifestado por la población), solo un 10% califica a la mencionada dimensión en un nivel medianamente satisfactorio.

Finalmente, respecto a la dimensión desarrollo, se observa que el 60% de la población, califica a la mencionada dimensión en un nivel ineficiente, mientras tanto solo 20% manifiesta que se encuentra en un nivel medianamente satisfactorio.

A continuación, se desglosan los niveles de las dimensiones de la auditoría informática:

DIMENSIÓN PRELIMINAR

Tabla 2. Niveles de la dimensión preliminar

Nivel de auditoria	**Frecuencia**	**Porcentaje válido**
Ineficiente	7	70.0%
Inicio	2	20.0%
Medianamente satisfactorio	1	10.0%
Eficiente y satisfactorio	0	0.0%
Total	10	100%

Fuente: Tabla 1

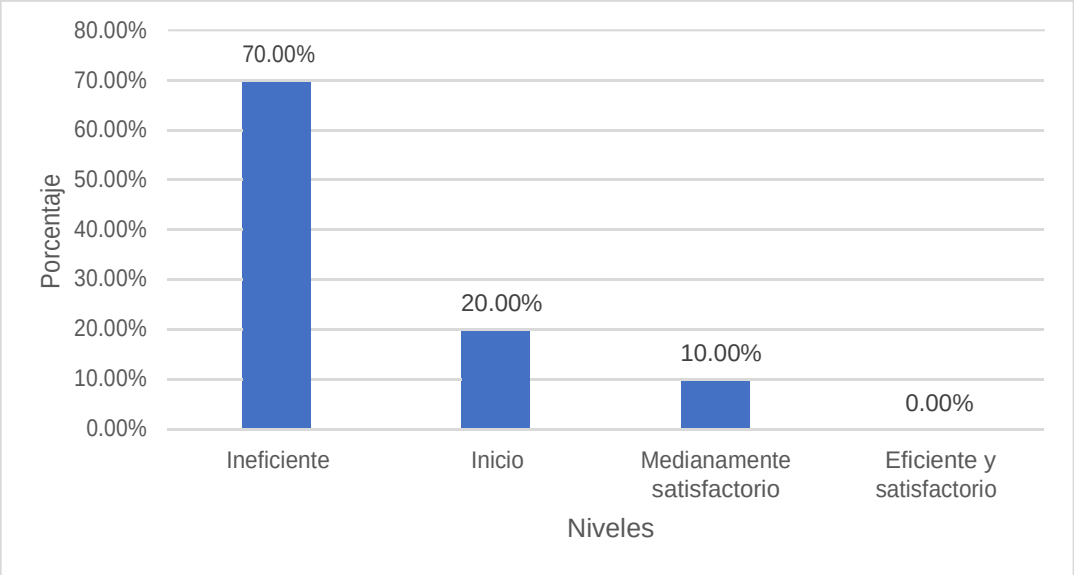


Figura 2: Niveles de la dimensión preliminar

Fuente: Tabla 2

En la Tabla y figura 2, se observa que la dimensión preliminar se encuentra en un nivel ineficiente, manifestado por el 70% de la población, mientas tanto solo el 10% califica dicha dimensión en un nivel medianamente satisfactorio.

DIMENSIÓN JUSTIFICACIÓN

Tabla 3. Niveles de la dimensión justificación

Nivel de auditoria	Frecuencia	Porcentaje válido
Ineficiente	8	80.00%
Inicio	1	10.00%
Medianamente satisfactorio	1	10.00%
Eficiente y satisfactorio	0	0.00%
Total	10	100%

Fuente: Instrumento aplicado

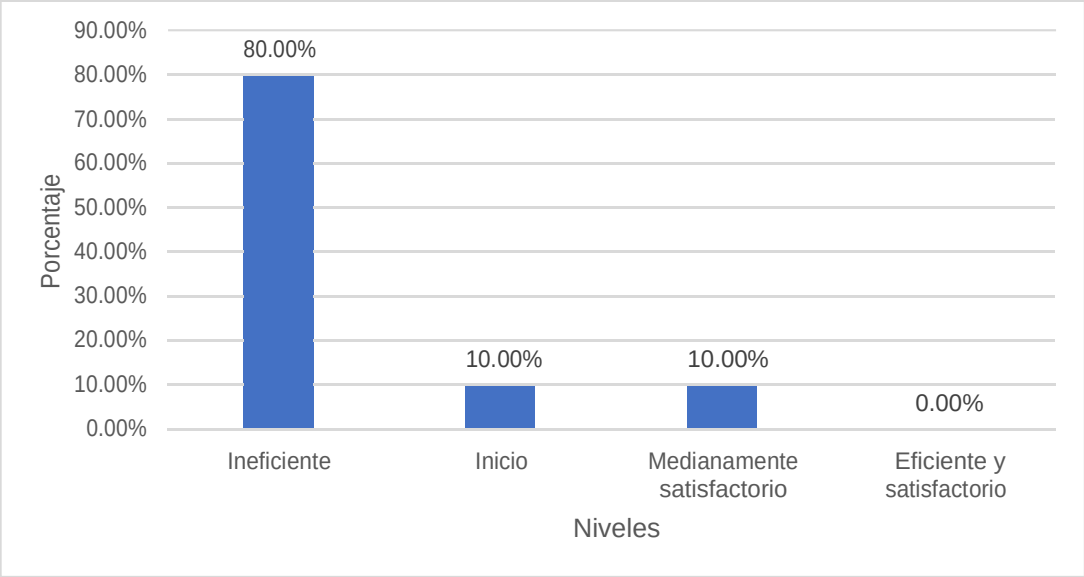


Figura 3: Niveles de la dimensión justificación

Fuente: Tabla 3

En la Tabla y Figura 3, se demuestra que la dimensión justificación se encuentra en un nivel ineficiente, manifestado por el 80% de la población encuestada y solo el 10% la califica en un nivel medianamente satisfactorio.

DIMENSIÓN ADECUACIÓN

Tabla 4. Niveles de la dimensión adecuación

Nivel de auditoria	Frecuencia	Porcentaje válido
Ineficiente	4	40.00%
Inicio	3	30.00%
Medianamente satisfactorio	3	30.00%
Eficiente y satisfactorio	0	0.00%
Total	10	100%

Fuente: Instrumento aplicado

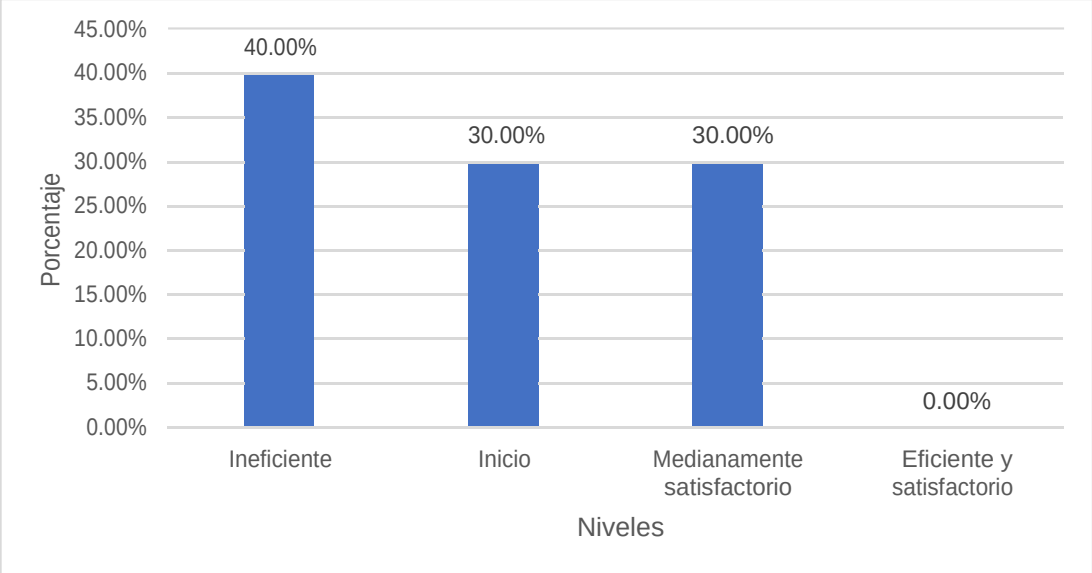


Figura 4: Niveles de la dimensión adecuación

Fuente: Tabla 4

En la Tabla y Figura 4, se observa que la dimensión adecuación, se encuentra en un nivel ineficiente, manifestado por el 40% de la población, mientras tanto un 30% y 30% de la población, la califica en niveles de inicio y medianamente satisfactorio.

DIMENSIÓN FORMALIZACIÓN

Tabla 5. Niveles de la dimensión formalización

Nivel de auditoria	Frecuencia	Porcentaje válido
Ineficiente	7	70.00%
Inicio	2	20.00%
Medianamente satisfactorio	1	10.00%
Eficiente y satisfactorio	0	0.00%
Total	10	100%

Fuente: Instrumento aplicado

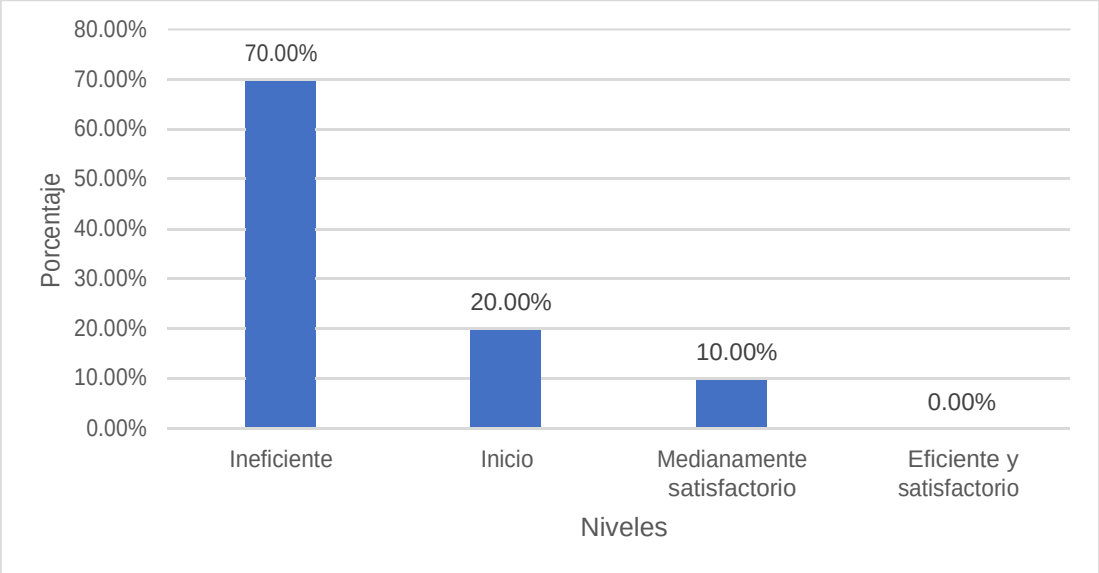


Figura 5: Niveles de la dimensión formalización

Fuente: Tabla 5

Se observa en la Tabla y Figura 5, que la dimensión formalización se encuentra en un nivel ineficiente, manifestado por el 70% de la población encuestado, mientras tanto solo el 10% la califica en un nivel medianamente satisfactorio.

DIMENSIÓN DESARROLLO

Tabla 6. Niveles de la dimensión desarrollo

Nivel de auditoria	Frecuencia	Porcentaje válido
Ineficiente	6	60.00%
Inicio	2	20.00%
Medianamente satisfactorio	2	20.00%
Eficiente y satisfactorio	0	0.00%
Total	10	100%

Fuente: Instrumento aplicación

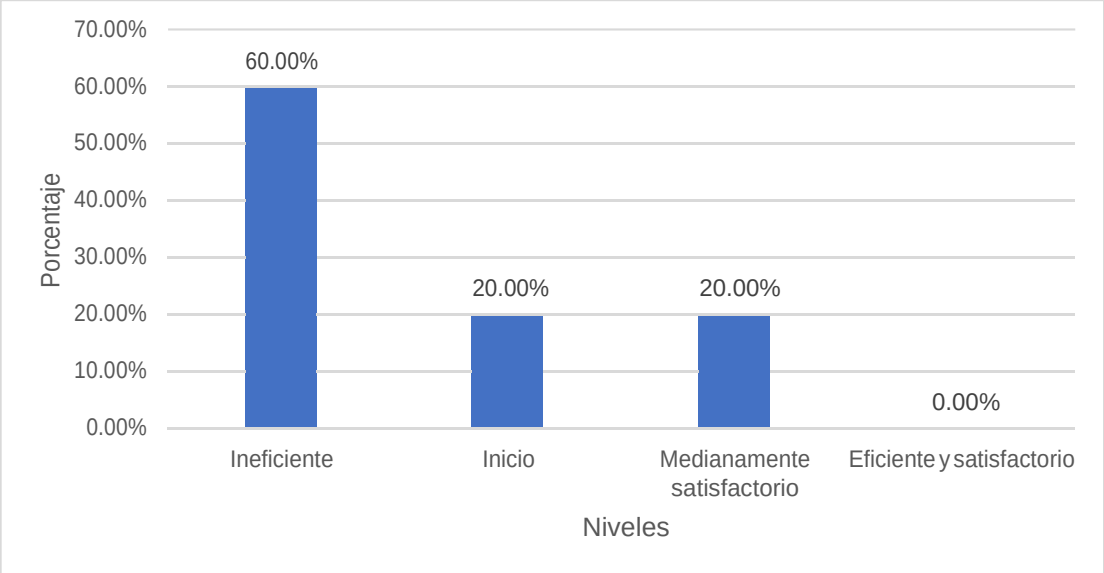


Figura 6: Niveles de la dimensión desarrollo
Fuente: Tabla 6

En la Tabla y Figura 6, se observa que la dimensión desarrollo se encuentra en un nivel ineficiente, manifestado por el 60% de la población, mientras tanto el 20% y 20% la califica en un nivel de inicio y medianamente satisfactorio.

VARIABLE SEGURIDAD DE LA INFORMACIÓN

A continuación, se presenta los niveles de las dimensiones de la seguridad de la información:

Tabla 7. Niveles de las dimensiones de la seguridad de la información

DIMENSIONES DE LA SEGURIDAD DE LA INFORMACIÓN			
NIVELES	**CONFIABILIDAD**	**INTEGRIDAD**	**DISPONIBILIDAD**
Seguridad ineficiente	40.00%	30.00%	20.00%
Seguridad en inicio	30.00%	40.00%	40.00%
Seguridad medianamente satisfactorio	30.00%	30.00%	40.00%
Seguridad y satisfactorio	0.00%	0.00%	0.00%

Fuente: Instrumento aplicado (Anexo 2)

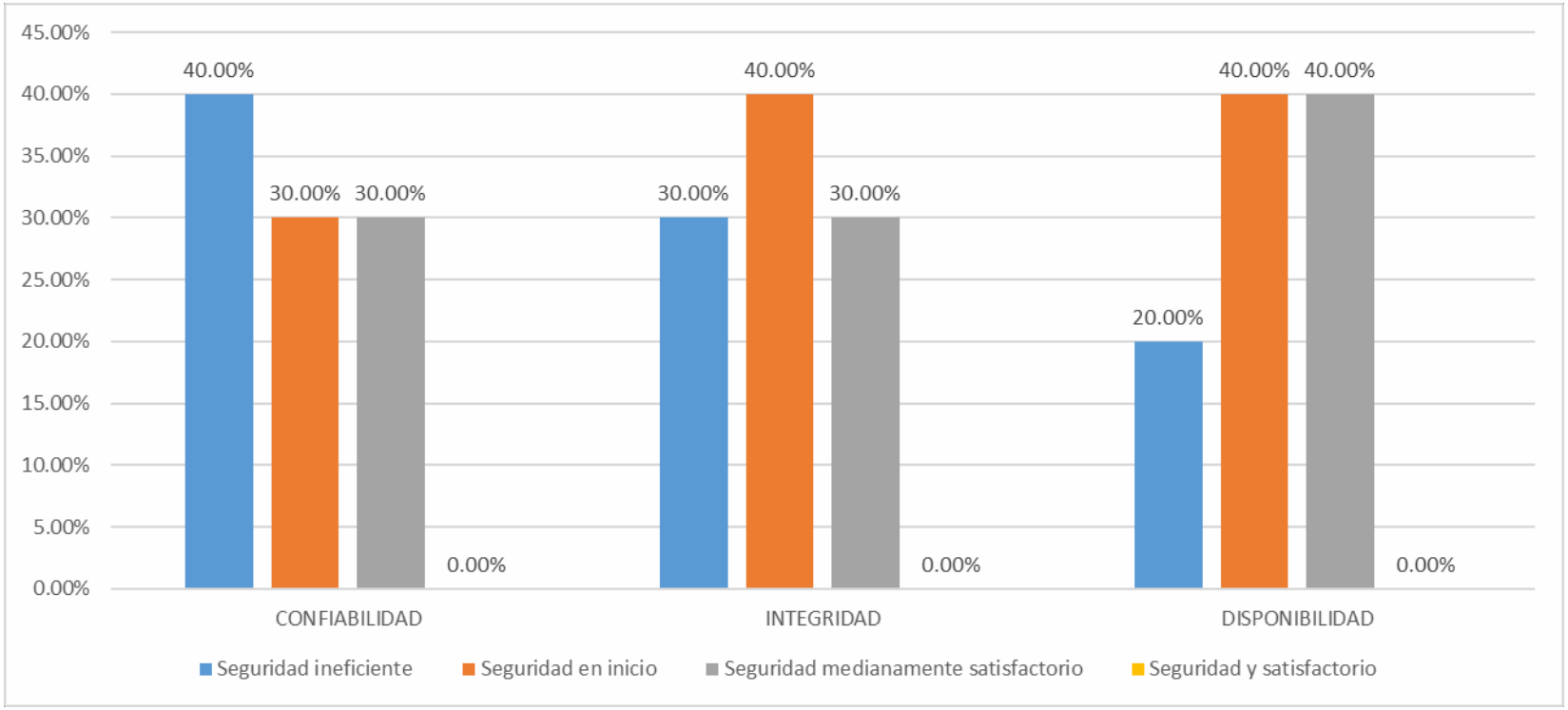


Figura 7: Niveles de las dimensiones de la seguridad informática

Fuente: Tabla 7

En la Tabla y Figura 7 se observa respecto a las dimensiones de la seguridad informática, en cuanto a la dimensión confiabilidad, la misma se encuentra en un nivel ineficiente, validado por el 40% de la población encuestada, mientras tanto un considerable grupo conformado por el 30%, manifiesta que encuentra en un nivel medianamente satisfactorio. Por otro lado, para el caso de la dimensión integridad, se denota que el 40% de la población encuestada, manifiesta que la mencionada dimensión se encuentra en un nivel de inicio, mientras tanto un 30% la califica en un nivel ineficiente.

Finalmente, respecto a la dimensión disponibilidad, se observa que el 40% de la población, califica a la mencionada dimensión en un nivel medianamente satisfactorio, mientras tanto solo 20% manifiesta que se encuentra en un nivel ineficiente.

Dimensión confiabilidad

Tabla 8. Niveles de la dimensión confiabilidad

Nivel de seguridad	Frecuencia	Porcentaje válido
Seguridad ineficiente	4	40.00%
Seguridad en inicio	3	30.00%
Seguridad medianamente satisfactorio	3	30.00%
Seguridad eficiente y satisfactorio	0	0.00%
Total	10	100%

Fuente: Instrumento aplicado (Anexo 2)

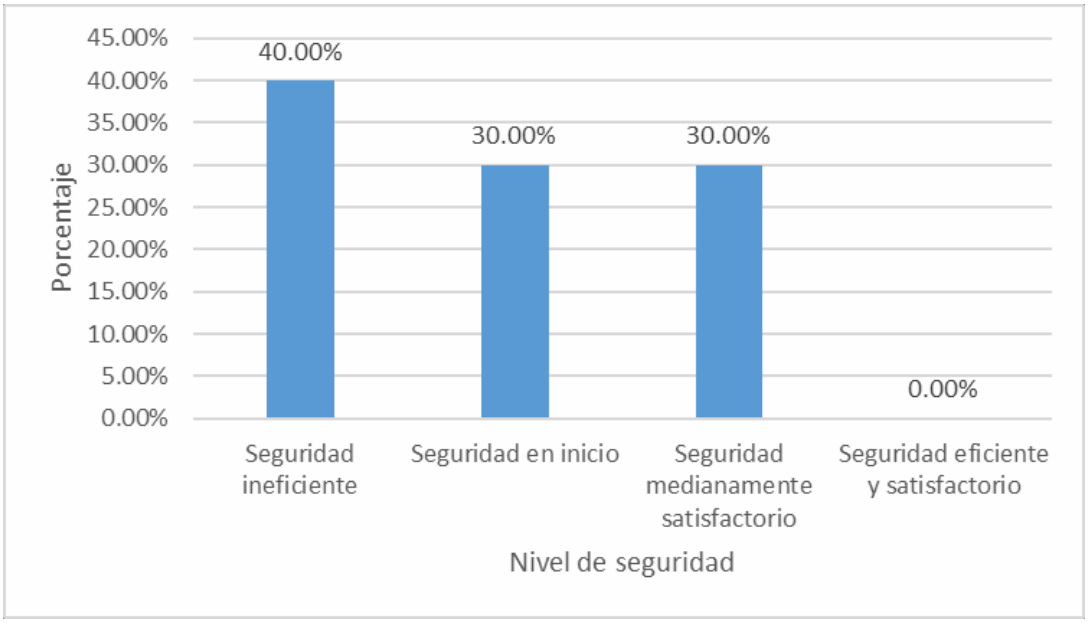


Figura 8: Niveles de la dimensión confiabilidad
Fuente: Tabla 8

En la Tabla y Figura 8, se observa que la dimensión confiabilidad se encuentra en un nivel ineficiente, manifestado por el 40% de la población, mientras tanto un considerable grupo conformado por el 30%, la califica en un nivel de seguridad medianamente satisfactorio.

Dimensión integridad

Tabla 9. Niveles de la dimensión integridad

Nivel de seguridad	Frecuencia	Porcentaje válido
Seguridad ineficiente	3	30.00%
Seguridad en inicio	4	40.00%
Seguridad medianamente satisfactorio	3	30.00%
Seguridad eficiente y satisfactorio	0	0.00%
Total	10	100%

Fuente: Instrumento aplicado (Anexo 2)

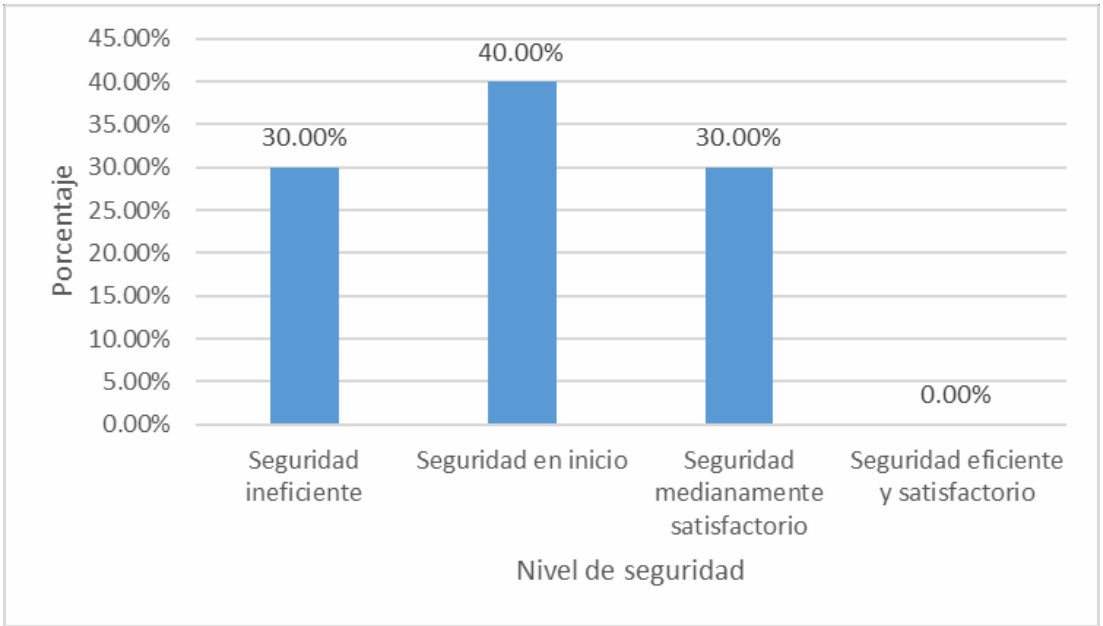


Figura 9: Niveles de la dimensión integridad
Fuente: Tabla 9

En la Tabla y Figura 9, se observa que la dimensión integridad, se encuentra en un nivel de seguridad en inicio, manifestado por el 40% de la población, mientras tanto un 30% la califica en un nivel de seguridad ineficiente.

Dimensión Disponibilidad

Tabla 10. Niveles de la dimensión disponibilidad

Nivel de seguridad	Frecuencia	Porcentaje válido
Seguridad ineficiente	2	20.00%
Seguridad en inicio	4	40.00%
Seguridad medianamente satisfactorio	4	40.00%
Seguridad eficiente y satisfactorio	0	0.00%
Total	10	100%

Fuente: Instrumento aplicado (Anexo 2)

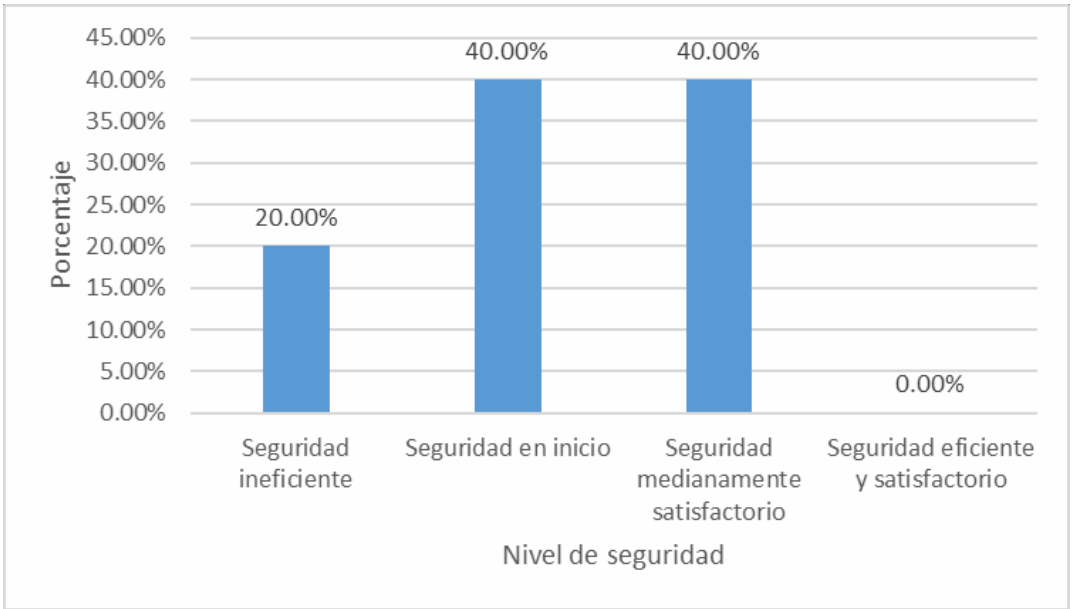


Figura 10: Niveles de la dimensión integridad
Fuente: Tabla 10

En la Tabla y Figura 6, se observa que la dimensión integridad se encuentra en un nivel de seguridad en inicio y medianamente satisfactorio, manifestado por el 40% y 40% de la población respectivamente, mientras tanto solo el 20% la califica en un nivel ineficiente.

Tabla 11. Coeficiente de correlación entre la auditoria informática y la seguridad de la información

		Nivel de auditoria informática	Nivel de seguridad de la información
Nivel de auditoria informática	Correlación de Pearson	1	,640*
	Sig. (bilateral)		,009
	N	10	10
Nivel de seguridad de la información	Correlación de Pearson	,640*	1
	Sig. (bilateral)	,009	
	N	10	10

*. La correlación es significativa en el nivel 0,01 (bilateral).

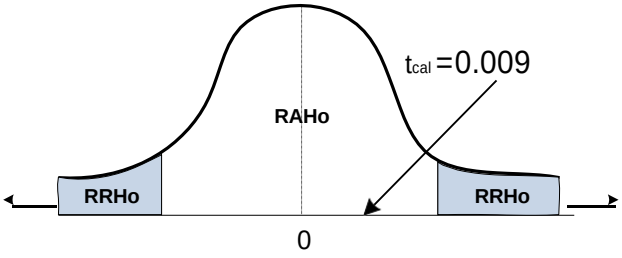
Fuente: Tabla 1 y 7

En la Tabla 10 se pueden observar una correlación R de Pearson moderada de 0.640, significativa al 1% (0.009), por lo tanto, con los resultados obtenidos, se acepta la hipótesis que establece que la auditoría informática se relaciona significativamente con la seguridad de la información en el área de sistemas de la Caja del Santa, Chimbote 2018

Contrastación de hipótesis

H: La auditoría informática se relaciona significativamente con la seguridad de la información en el área de sistemas de la Caja del Santa, Chimbote 2018	
Hipótesis estadística	Nivel de significancia (α)
Si: $r_{xy} = 0$; $t_{cal} < t_{tab} \Rightarrow$ Se acepta la H. r_{xy} = ···.; …. < 0.009	α = 0.05

Curva de Gauss



VIII. DISCUSIÓN

En este apartado se someterá a discusión los resultados obtenidos, realizando una comparación los resultados a los que han llegado en las investigaciones detalladas como antecedentes de investigación. Respecto a los resultados obtenidos, se acepta la hipótesis de investigación.

Respecto a las dimensiones de la auditoría informática, en cuanto a la dimensión preliminar, la misma se encontró en un nivel ineficiente, validado por el 70% de la población encuestada, por otro lado, para el caso de la dimensión justificación, se denota que más de la mitad, es decir el 80% de la población encuestada, manifiesta que la mencionada dimensión se encuentra en un nivel ineficiente, en cuanto a la dimensión adecuación, el 40% de la población manifiesta que se encuentra en un nivel de inicio y respecto a la dimensión formalización, se evidencia que se encuentra en un nivel ineficiente en un 70% (manifestado por la población), solo un 10% califica a la mencionada dimensión en un nivel medianamente satisfactorio. Finalmente, respecto a la dimensión desarrollo, se observa que el 60% de la población, califica a la mencionada dimensión en un nivel ineficiente; por lo que se pudo denotar, la auditoría informática en la institución objeto de estudio aún se encuentra en un nivel bajo, no habiéndose implementado los procesos básicos que exige la misma para la seguridad de la información, dichos procesos son explicados en Apuntes de Auditoría Informática (2009), donde se afirma que dentro del proceso de auditoría es importante asegurar que se cumplan por lo menos los principios básicos de un proceso formal. Los elementos indispensables para cumplir este requisito son: la planeación, el control y el seguimiento del desempeño; por lo tanto, actualmente no se evidencia dicho escenario.

En la Tabla 7, respecto a las dimensiones de la seguridad informática, en cuanto a la dimensión confiabilidad, la misma se encuentra en un nivel ineficiente, validado por el 40% de la población encuestada; por otro lado, para el caso de la dimensión integridad, se denota que el 40% de la población encuestada, manifiesta que la mencionada dimensión se encuentra en un nivel de inicio y finalmente, respecto a la dimensión disponibilidad, se observa que el 40% de la población, califica a la mencionada dimensión en un nivel medianamente satisfactorio, ante ello se

postula lo manifestado por la ISO (2005), un sistema de seguridad de información es un conjunto de responsabilidades, procesos, procedimientos y recursos que establece la alta dirección con el propósito de dirigir y controlar la seguridad de los activos de información y asegurar la continuidad de la operatividad de la empresa.

Finalmente, en la Tabla 10 se pueden observar una correlación R de Pearson moderada de 0.640, significativa al 1% (0.009), por lo tanto, con los resultados obtenidos, se acepta la hipótesis que establece que la auditoría informática se relaciona significativamente con la seguridad de la información en el área de sistemas de la Caja del Santa, Chimbote 2018.

IX. CONCLUSIONES

Se Determinó en qué medida la auditoría informática se relaciona con la seguridad de la información en la Caja del Santa, lo cual se evidencia en:

1. Se identificó el nivel de auditoría informática por sus dimensiones, lográndose manifestar en cuanto a la dimensión preliminar, que la misma se encuentra en un nivel ineficiente, validado por el 70% de la población encuestada, para el caso de la dimensión justificación, se denota que más de la mitad, es decir el 80% de la población encuestada, manifiesta que la mencionada dimensión se encuentra en un nivel ineficiente; en cuanto a la dimensión adecuación, el 40% de la población manifiesta que se encuentra en un nivel de inicio, respecto a la dimensión formalización, se evidencia que se encuentra en un nivel ineficiente en un 70% (manifestado por la población), finalmente, de igual modo, respecto a la dimensión desarrollo, se observa que el 60% de la población, califica a la mencionada dimensión en un nivel ineficiente.

2. Se determinó el nivel de la seguridad informática mediante sus dimensiones, donde para el caso de la dimensión confiabilidad se encontró en un nivel ineficiente, validado por el 40% de la población encuestada, mientras tanto para el caso de la dimensión integridad, el 40% de la población encuestada, manifestó que la mencionada dimensión se encuentra en un nivel de inicio, finalmente, respecto a la dimensión disponibilidad, el 40% de la población, califica a la mencionada dimensión en un nivel medianamente satisfactorio.

3. Respecto al objetivo principal se obtuvo una correlación R de Pearson moderada de 0.640, significativa al 1% (0.009), por lo tanto, con ello se acepta la hipótesis que establece que la auditoría informática se relaciona significativamente con la seguridad de la información en el área de sistemas de la Caja del Santa, Chimbote 2018

X. RECOMENDACIONES

1. Establecer un comité de Tecnología de Información, con una participación activa de auditoria informática, en el que incluya prioritariamente dentro de su agenda, el desarrollo del plan estratégico de contingencia informática, así también, el personal del área de Tecnología de Información y el auditor informático deberán recibir una capacitación continua en la materia.

2. Cifrar toda información importante y complementaria de la empresa, en especial la información de los clientes; así mismo, establecer permisos al personal, con la finalidad de restringir accesos a los mismos, de tal forma que sólo el personal autorizado pueda acceder a información delicada de la empresa objeto de estudio, mediante documentos normativos.

3. Realizar una investigación de tipo experimental, con la finalidad de utilizar los resultados de la presente tesis como referencia, para implementar una propuesta de mejora de la seguridad de la información, mediante una metodología, que permita estructurar la propuesta de manera organizada y jerarquizada.

4. Ampliar la población de evaluación de la variable auditoría a los miembros de las gerencias ejecutivas, con la finalidad de identificar problemas raíces que esté afectando los procesos internos de la empresa.

XI. REFERENCIAS

Álvarez. Tesis de Magister en Ingeniería del Software: Asistente para la Realización de Auditorías de Sistemas en Organismos Públicos o Privados. 2015. España. Extraído de: http://laboratorios.fi.uba.ar/lsi/rgm/tesistas/kuna-tesisdemagister.pdf

Aguirre, Y. Propuesta de implantación del área de auditoría en informática en un órgano legislativo. Seminario de Auditoría Informática. s.f.

Auditoría Gubernamental. Técnicas de prácticas de auditoría. 2011. Extraído de http://www.slideshare.net/JOVIMECARCH/tecnicas-de-practicas-auditoriapresentation

Coronel, Karoly. Auditoria informática orientada a los procesos críticos de créditos generados en la Cooperativa Ahorro y Crédito Fortuna aplicando el marco de trabajo COBIT. Tesis de grado. Universidad Técnica Particular de Loja, Loja, Ecuador: s.n., 2013.

Carrizo. Auditoria Informática: Un Enfoque Metodológico y Práctico. México: Continental. 2013.

Jara, Sayuri. Auditoría informática de la gestión de ti para la empresa “Advance Consulting” utilizando el modelo COBIT. Tesis de grado. Pontificia Universidad Católica de Ecuador, Quito, Ecuador: s.n., 2013.

Nazareno, Génesis. Auditoría informática en el área administrativa de la pontificia universidad católica del ecuador sede esmeraldas. Tesis de grado. Pontificia Universidad Católica de Ecuador, Quito, Ecuador: s.n., 2016.

Ramos, Carmen. Propuesta de un plan de auditoria informática para el "sistema de información en salud" y el "aplicativo para el registro de formatos SIS" en los establecimientos de salud de la unidad ejecutora 400 en la región Piura en el año 2015. Tesis de grado. Universidad Nacional de Piura, Piura, Perú: s.n.

Vanegas. Auditoria Informática: Un Enfoque Práctico. España: computec RAMA. 2016.

Ziegler, R. Auditoria Moderna. Continental. s.f.

XII. ANEXOS

ANEXO 1

CUESTIONARIO PARA USUARIOS SOBRE LA AUDITORIA INFORMATICA EN EL AREA DE SISTEMAS DE LA CAJA DEL SANTA

	ESCALAS			
DIMENSIONES	**NO APLICA**	**CASI SE APLICA**	**APLICA REGULARMENTE**	**APLICA**
PRELIMINAR				
Definición del plan estratégico de TI				
Definición de la arquitectura de la información				
Determinación de la dirección tecnológica.				
Definición de los procesos, organización y relaciones de TI.				
JUSTIFICACION				
Administración de la inversión en TI				
Comunicación con la Alta Dirección				
Administración de los recursos humanos de TI.				
Administración de la calidad de TI				
Evaluación y administración de los riesgos de TI.				
Administración de los proyectos de TI				
ADECUACION				
Identificación de las soluciones automatizadas				
Adquisición y mantenimiento del software aplicativo				
Adquisición y mantenimiento de la infraestructura tecnológica				
Facilitad de operación y uso de TI				
Adquisición de recursos de TI				
Administración de cambios en TI				
Instalación y acreditación de soluciones y cambios en TI				
FORMALIZACION				
Definición y administración de los niveles de servicio				
Administración de los servicios de terceros				
Administración del desempeño y capacidad de TI				
Garantías en la continuidad del servicio				
Garantías en la seguridad de los sistemas				
Identificación y asignación de costos de TI				
Educación y entrenamiento a los usuarios				
Administración de la mesa de servicios de TI y los incidentes				

Administración de la configuración de TI
Administración de los problemas con TI
Administración de los datos
Administración del ambiente físico
Administración de las operaciones de TI
DESARROLLO
Monitoreo y evaluación del desempeño de TI
Monitoreo y evaluación el control interno
Garantías en el cumplimiento regulatorio
Proporciona gobierno de TI

BAREMOS

PRELIMINAR	
0 AL 5	INEFICIENTE
6 AL 9	EN INICIO
10 AL 13	MEDIANAMENTE SATISFACTORIO
14 AL 16	EFICIENTE Y SATISFACTORIO

JUSTIFICACION	
0 AL 10	INEFICIENTE
11 AL 14	EN INICIO
15 AL 19	MEDIANAMENTE SATISFACTORIO
20 AL 24	EFICIENTE Y SATISFACTORIO

ADECUACION	
0 AL 10	INEFICIENTE
11 AL 17	EN INICIO
18 AL 23	MEDIANAMENTE SATISFACTORIO
24 AL 28	EFICIENTE Y SATISFACTORIO

FORMALIZACION	
0 AL 20	INEFICIENTE
21 AL 30	EN INICIO
31 AL 40	MEDIANAMENTE SATISFACTORIO
41 AL 52	EFICIENTE Y SATISFACTORIO

DESARROLLO	
0 AL 5	INEFICIENTE
6 AL 9	EN INICIO
10 AL 13	MEDIANAMENTE SATISFACTORIO
14 AL 16	EFICIENTE Y SATISFACTORIO

ANEXO 2

CUESTIONARIO PARA USUARIOS SOBRE LA SEGURIDAD DE LA INFORMACIÓN EN EL AREA DE SISTEMAS DE LA CAJA DEL SANTA

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
CONFIABILIDAD				
Control de las actividades de los equipo de computación				
Control del uso de los equipos				
Cambios, modificaciones o nuevo software cuentan con autorización de la gerencia				
Usuarios cuentan con una especificación sobre los programas que pueden acceder según sea su cargo dentro de la empresa				
Políticas frente a la propiedad intelectual y derechos de autor en la implantación y uso de software en la empresa				
INTEGRIDAD				
Se solicita a usuarios la respectiva autenticación en la red inalámbrica				
La red esta provista de FIREWALL adicional al incorporado en los sistemas operativos a fin de detectar y neutralizar la presencia de intrusos o hackers en la red				
Se lleva un registro de los mensajes lógicos de transmisión los cuales has de constar el origen, fecha, hora y receptor				
Se efectúa un registro aleatorio de las actividades de los usuarios de la red a fin de determinar los hábitos frecuentes de los mismos y detectar supuestas colaboraciones con terceros en el robo de información				
DISPONIBILIDAD				
Planificación adecuada para el mantenimiento de los equipos				
Manual de procedimientos de mantenimiento del hardware				
Sistemas operativos aplicaciones y paquetes utilitarios cuentan con licencia original				
Las fallas en los programas son documentadas y revisadas adecuadamente				
Existencia de programas actualizados de antivirus con el fin de evitar que los computadores presenten deficiencias en su funcionamiento lógico				
Se propone un proceso de evaluación previo al sistema para de esta manera poder interactuar mejor con el sistema principal				
Se indica un test a usuarios para promover mejor la utilización del software de la empresa				

BAREMOS

CONFIABILIDAD	
0 AL 7	SEGURIDAD INEFICIENTE
8 AL 11	SEGURIDAD EN INICIO
12 AL 14	SEGURIDAD MEDIANAMENTE SATISFACTORIO
15 AL 20	SEGURIDAD EFICIENTE Y SATISFACTORIO

PRELIMINAR	
0 AL 5	SEGURIDAD INEFICIENTE
6 AL 9	SEGURIDAD EN INICIO
10 AL 13	SEGURIDAD MEDIANAMENTE SATISFACTORIO
14 AL 16	SEGURIDAD EFICIENTE Y SATISFACTORIO

DISPONIBILIDAD	
0 AL 10	SEGURIDAD INEFICIENTE
11 AL 17	SEGURIDAD EN INICIO
18 AL 23	SEGURIDAD MEDIANAMENTE SATISFACTORIO
24 AL 28	SEGURIDAD EFICIENTE Y SATISFACTORIO

ANEXO 3

FICHA TÉCNICA DEL UNIVERSO POBLACIONAL

EMPRESA/AREA ENCUESTADA: CAJA DEL SANTA / AREA DE SISTEMAS.

UNIVERSO: Personas involucradas en la auditoria informática realizada en el área de sistemas de la empresa Caja del Santa, exceptuando aquellas personas que se encuentran laborando en otras áreas.

TAMAÑO Y DISTRIBUCIÓN DE LA MUESTRA: 20 cuestionarios distribuidos entre los siguientes cargos del área objeto de estudio:

Cargos del área de Sistemas	Cantidad de trabajadores
- Jefe de tecnología	1
- Analista funcional	1
- Analista desarrollador	1
- Administrador de red	1
- Administrador de base de datos	1
- Analista de control de calidad	1
- Asistente de red	1
- Asistente de soporte técnico	1
- Asistente de base de datos	1
- Analista de inteligencia de negocios	1
Total	10

TÉCNICA DE RECOLECCIÓN DE DATOS: Encuestas cara a cara en el área objeto de estudio.

FECHA DE RECOLECCIÓN DE LOS DATOS: Del 02 de diciembre al 15 de diciembre del 2017, el mismo fue realizado por el responsable del presente informe.

TEMAS A LOS QUE SE REFIERE: Determinar la percepción que tiene el impacto de la auditoria informática en la seguridad de la información.

Analizar diferencias en las percepciones de los diferentes trabajadores que participaron en la auditoría informática que se realizó en la empresa objeto de estudio.

PREGUNTAS CONCRETAS QUE SE FORMULARON: referirse a cuestionario.

ANEXO 04

BASE DE DATOS DE LA VARIABLE AUDITORIA INFORMÁTICA

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
PRELIMINAR				
Definición del plan estratégico de TI	X			
Definición de la arquitectura de la información	X			
Determinación de la dirección tecnológica.	X			
Definición de los procesos, organización y relaciones de TI.		X		
JUSTIFICACION				
Administración de la inversión en TI	X			
Comunicación con la Alta Dirección	X			
Administración de los recursos humanos de TI.	X			
Administración de la calidad de TI	X			
Evaluación y administración de los riesgos de TI.		X		
Administración de los proyectos de TI		X		
ADECUACION				
Identificación de las soluciones automatizadas	X			
Adquisición y mantenimiento del software aplicativo	X			
Adquisición y mantenimiento de la infraestructura tecnológica	X			
Facilitad de operación y uso de TI		X		
Adquisición de recursos de TI		X		
Administración de cambios en TI		X		
Instalación y acreditación de soluciones y cambios en TI	X			
FORMALIZACION				
Definición y administración de los niveles de servicio	X			
Administración de los servicios de terceros	X			
Administración del desempeño y capacidad de TI	X			
Garantías en la continuidad del servicio	X			
Garantías en la seguridad de los sistemas	X			
Identificación y asignación de costos de TI	X			
Educación y entrenamiento a los usuarios	X			
Administración de la mesa de servicios de TI y los incidentes	X			
Administración de la configuración de TI		X		
Administración de los problemas con TI		X		
Administración de los datos		X		
Administración del ambiente físico		X		
Administración de las operaciones de TI		X		

DESARROLLO				
Monitoreo y evaluación del desempeño de TI	X			
Monitoreo y evaluación el control interno	X			
Garantías en el cumplimiento regulatorio	X			
Proporciona gobierno de TI	X			

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
PRELIMINAR				
Definición del plan estratégico de TI	X			
Definición de la arquitectura de la información		X		
Determinación de la dirección tecnológica.	X			
Definición de los procesos, organización y relaciones de TI.	X			
JUSTIFICACION				
Administración de la inversión en TI	X			
Comunicación con la Alta Dirección	X			
Administración de los recursos humanos de TI.	X			
Administración de la calidad de TI		X		
Evaluación y administración de los riesgos de TI.	X			
Administración de los proyectos de TI	X			
ADECUACION				
Identificación de las soluciones automatizadas	X			
Adquisición y mantenimiento del software aplicativo	X			
Adquisición y mantenimiento de la infraestructura tecnológica	X			
Facilitad de operación y uso de TI		X		
Adquisición de recursos de TI		X		
Administración de cambios en TI		X		
Instalación y acreditación de soluciones y cambios en TI	X			
FORMALIZACION				
Definición y administración de los niveles de servicio	X			
Administración de los servicios de terceros	X			
Administración del desempeño y capacidad de TI	X			
Garantías en la continuidad del servicio	X			
Garantías en la seguridad de los sistemas	X			
Identificación y asignación de costos de TI	X			
Educación y entrenamiento a los usuarios	X			
Administración de la mesa de servicios de TI y los incidentes	X			
Administración de la configuración de TI		X		
Administración de los problemas con TI		X		
Administración de los datos		X		
Administración del ambiente físico		X		
Administración de las operaciones de TI		X		
DESARROLLO				
Monitoreo y evaluación del desempeño de TI	X			
Monitoreo y evaluación el control interno	X			
Garantías en el cumplimiento regulatorio	X			

Proporciona gobierno de TI		X		

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
PRELIMINAR				
Definición del plan estratégico de TI	X			
Definición de la arquitectura de la información	X			
Determinación de la dirección tecnológica.	X			
Definición de los procesos, organización y relaciones de TI.		X		
JUSTIFICACION				
Administración de la inversión en TI	X			
Comunicación con la Alta Dirección	X			
Administración de los recursos humanos de TI.	X			
Administración de la calidad de TI	X			
Evaluación y administración de los riesgos de TI.		X		
Administración de los proyectos de TI		X		
ADECUACION				
Identificación de las soluciones automatizadas	X			
Adquisición y mantenimiento del software aplicativo	X			
Adquisición y mantenimiento de la infraestructura tecnológica	X			
Facilitad de operación y uso de TI	X			
Adquisición de recursos de TI		X		
Administración de cambios en TI		X		
Instalación y acreditación de soluciones y cambios en TI	X			
FORMALIZACION				
Definición y administración de los niveles de servicio	X			
Administración de los servicios de terceros	X			
Administración del desempeño y capacidad de TI	X			
Garantías en la continuidad del servicio	X			
Garantías en la seguridad de los sistemas	X			
Identificación y asignación de costos de TI	X			
Educación y entrenamiento a los usuarios		X		
Administración de la mesa de servicios de TI y los incidentes		X		
Administración de la configuración de TI		X		
Administración de los problemas con TI		X		
Administración de los datos	X			
Administración del ambiente físico	X			
Administración de las operaciones de TI	X			
DESARROLLO				
Monitoreo y evaluación del desempeño de TI	X			
Monitoreo y evaluación el control interno	X			
Garantías en el cumplimiento regulatorio	X			

Proporciona gobierno de TI		X		

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
PRELIMINAR				
Definición del plan estratégico de TI	X			
Definición de la arquitectura de la información		X		
Determinación de la dirección tecnológica.	X			
Definición de los procesos, organización y relaciones de TI.	X			
JUSTIFICACION				
Administración de la inversión en TI	X			
Comunicación con la Alta Dirección	X			
Administración de los recursos humanos de TI.	X			
Administración de la calidad de TI	X			
Evaluación y administración de los riesgos de TI.		X		
Administración de los proyectos de TI		X		
ADECUACION				
Identificación de las soluciones automatizadas	X			
Adquisición y mantenimiento del software aplicativo	X			
Adquisición y mantenimiento de la infraestructura tecnológica		X		
Facilitad de operación y uso de TI		X		
Adquisición de recursos de TI		X		
Administración de cambios en TI	X			
Instalación y acreditación de soluciones y cambios en TI	X			
FORMALIZACION				
Definición y administración de los niveles de servicio	X			
Administración de los servicios de terceros	X			
Administración del desempeño y capacidad de TI	X			
Garantías en la continuidad del servicio	X			
Garantías en la seguridad de los sistemas	X			
Identificación y asignación de costos de TI	X			
Educación y entrenamiento a los usuarios	X			
Administración de la mesa de servicios de TI y los incidentes		X		
Administración de la configuración de TI		X		
Administración de los problemas con TI		X		
Administración de los datos	X			
Administración del ambiente físico	X			
Administración de las operaciones de TI		X		
DESARROLLO				
Monitoreo y evaluación del desempeño de TI	X			
Monitoreo y evaluación el control interno	X			
Garantías en el cumplimiento regulatorio	X			

Proporciona gobierno de TI	X			

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
PRELIMINAR				
Definición del plan estratégico de TI	X			
Definición de la arquitectura de la información	X			
Determinación de la dirección tecnológica.	X			
Definición de los procesos, organización y relaciones de TI.	X			
JUSTIFICACION				
Administración de la inversión en TI	X			
Comunicación con la Alta Dirección	X			
Administración de los recursos humanos de TI.	X			
Administración de la calidad de TI		X		
Evaluación y administración de los riesgos de TI.		X		
Administración de los proyectos de TI		X		
ADECUACION				
Identificación de las soluciones automatizadas		X		
Adquisición y mantenimiento del software aplicativo		X		
Adquisición y mantenimiento de la infraestructura tecnológica		X		
Facilitad de operación y uso de TI			X	
Adquisición de recursos de TI		X		
Administración de cambios en TI			X	
Instalación y acreditación de soluciones y cambios en TI		X		
FORMALIZACION				
Definición y administración de los niveles de servicio	X			
Administración de los servicios de terceros	X			
Administración del desempeño y capacidad de TI	X			
Garantías en la continuidad del servicio	X			
Garantías en la seguridad de los sistemas	X			
Identificación y asignación de costos de TI	X			
Educación y entrenamiento a los usuarios	X			
Administración de la mesa de servicios de TI y los incidentes		X		
Administración de la configuración de TI		X		
Administración de los problemas con TI		X		
Administración de los datos		X		
Administración del ambiente físico		X		
Administración de las operaciones de TI		X		
DESARROLLO				
Monitoreo y evaluación del desempeño de TI	X			
Monitoreo y evaluación el control interno	X			
Garantías en el cumplimiento regulatorio	X			

Proporciona gobierno de TI	X			

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
PRELIMINAR				
Definición del plan estratégico de TI	X			
Definición de la arquitectura de la información		X		
Determinación de la dirección tecnológica.	X			
Definición de los procesos, organización y relaciones de TI.	X			
JUSTIFICACION				
Administración de la inversión en TI		X		
Comunicación con la Alta Dirección		X		
Administración de los recursos humanos de TI.	X			
Administración de la calidad de TI	X			
Evaluación y administración de los riesgos de TI.	X			
Administración de los proyectos de TI		X		
ADECUACION				
Identificación de las soluciones automatizadas		X		
Adquisición y mantenimiento del software aplicativo		X		
Adquisición y mantenimiento de la infraestructura tecnológica		X		
Facilitad de operación y uso de TI		X		
Adquisición de recursos de TI		X		
Administración de cambios en TI			X	
Instalación y acreditación de soluciones y cambios en TI			X	
FORMALIZACION				
Definición y administración de los niveles de servicio	X			
Administración de los servicios de terceros	X			
Administración del desempeño y capacidad de TI	X			
Garantías en la continuidad del servicio	X			
Garantías en la seguridad de los sistemas	X			
Identificación y asignación de costos de TI	X			
Educación y entrenamiento a los usuarios	X			
Administración de la mesa de servicios de TI y los incidentes		X		
Administración de la configuración de TI		X		
Administración de los problemas con TI		X		
Administración de los datos		X		
Administración del ambiente físico		X		
Administración de las operaciones de TI	X			
DESARROLLO				
Monitoreo y evaluación del desempeño de TI		X		
Monitoreo y evaluación el control interno	X			
Garantías en el cumplimiento regulatorio	X			

Proporciona gobierno de TI	X			

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
PRELIMINAR				
Definición del plan estratégico de TI	X			
Definición de la arquitectura de la información		X		
Determinación de la dirección tecnológica.	X			
Definición de los procesos, organización y relaciones de TI.	X			
JUSTIFICACION				
Administración de la inversión en TI	X			
Comunicación con la Alta Dirección	X			
Administración de los recursos humanos de TI.	X			
Administración de la calidad de TI	X			
Evaluación y administración de los riesgos de TI.	X			
Administración de los proyectos de TI	X			
ADECUACION				
Identificación de las soluciones automatizadas		X		
Adquisición y mantenimiento del software aplicativo		X		
Adquisición y mantenimiento de la infraestructura tecnológica		X		
Facilitad de operación y uso de TI		X		
Adquisición de recursos de TI		X		
Administración de cambios en TI			X	
Instalación y acreditación de soluciones y cambios en TI		X		
FORMALIZACION				
Definición y administración de los niveles de servicio	X			
Administración de los servicios de terceros	X			
Administración del desempeño y capacidad de TI		X		
Garantías en la continuidad del servicio		X		
Garantías en la seguridad de los sistemas		X		
Identificación y asignación de costos de TI		X		
Educación y entrenamiento a los usuarios		X		
Administración de la mesa de servicios de TI y los incidentes		X		
Administración de la configuración de TI	X			
Administración de los problemas con TI	X			
Administración de los datos	X			
Administración del ambiente físico	X			
Administración de las operaciones de TI	X			
DESARROLLO				
Monitoreo y evaluación del desempeño de TI		X		
Monitoreo y evaluación el control interno		X		
Garantías en el cumplimiento regulatorio		X		

Proporciona gobierno de TI			X	

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
PRELIMINAR				
Definición del plan estratégico de TI	X			
Definición de la arquitectura de la información		X		
Determinación de la dirección tecnológica.		X		
Definición de los procesos, organización y relaciones de TI.		X		
JUSTIFICACION				
Administración de la inversión en TI	X			
Comunicación con la Alta Dirección	X			
Administración de los recursos humanos de TI.	X			
Administración de la calidad de TI	X			
Evaluación y administración de los riesgos de TI.	X			
Administración de los proyectos de TI		X		
ADECUACION				
Identificación de las soluciones automatizadas		X		
Adquisición y mantenimiento del software aplicativo		X		
Adquisición y mantenimiento de la infraestructura tecnológica			X	
Facilitad de operación y uso de TI			X	
Adquisición de recursos de TI		X		
Administración de cambios en TI			X	
Instalación y acreditación de soluciones y cambios en TI			X	
FORMALIZACION				
Definición y administración de los niveles de servicio		X		
Administración de los servicios de terceros		X		
Administración del desempeño y capacidad de TI		X		
Garantías en la continuidad del servicio		X		
Garantías en la seguridad de los sistemas		X		
Identificación y asignación de costos de TI		X		
Educación y entrenamiento a los usuarios		X		
Administración de la mesa de servicios de TI y los incidentes			X	
Administración de la configuración de TI			X	
Administración de los problemas con TI		X		
Administración de los datos		X		
Administración del ambiente físico	X			
Administración de las operaciones de TI		X		
DESARROLLO				
Monitoreo y evaluación del desempeño de TI			X	
Monitoreo y evaluación el control interno		X		
Garantías en el cumplimiento regulatorio		X		

Proporciona gobierno de TI		X		

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
PRELIMINAR				
Definición del plan estratégico de TI		X		
Definición de la arquitectura de la información		X		
Determinación de la dirección tecnológica.	X			
Definición de los procesos, organización y relaciones de TI.		X		
JUSTIFICACION				
Administración de la inversión en TI			X	
Comunicación con la Alta Dirección			X	
Administración de los recursos humanos de TI.			X	
Administración de la calidad de TI		X		
Evaluación y administración de los riesgos de TI.		X		
Administración de los proyectos de TI	X			
ADECUACION				
Identificación de las soluciones automatizadas		X		
Adquisición y mantenimiento del software aplicativo		X		
Adquisición y mantenimiento de la infraestructura tecnológica		X		
Facilitad de operación y uso de TI			X	
Adquisición de recursos de TI			X	
Administración de cambios en TI			X	
Instalación y acreditación de soluciones y cambios en TI			X	
FORMALIZACION				
Definición y administración de los niveles de servicio		X		
Administración de los servicios de terceros		X		
Administración del desempeño y capacidad de TI		X		
Garantías en la continuidad del servicio		X		
Garantías en la seguridad de los sistemas		X		
Identificación y asignación de costos de TI		X		
Educación y entrenamiento a los usuarios		X		
Administración de la mesa de servicios de TI y los incidentes		X		
Administración de la configuración de TI		X		
Administración de los problemas con TI			X	
Administración de los datos		X		
Administración del ambiente físico		X		
Administración de las operaciones de TI		X		
DESARROLLO				
Monitoreo y evaluación del desempeño de TI				
Monitoreo y evaluación el control interno			X	
Garantías en el cumplimiento regulatorio			X	

Proporciona gobierno de TI			X	

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
PRELIMINAR				
Definición del plan estratégico de TI			X	
Definición de la arquitectura de la información			X	
Determinación de la dirección tecnológica.			X	
Definición de los procesos, organización y relaciones de TI.		X		
JUSTIFICACION				
Administración de la inversión en TI			X	
Comunicación con la Alta Dirección			X	
Administración de los recursos humanos de TI.			X	
Administración de la calidad de TI			X	
Evaluación y administración de los riesgos de TI.				X
Administración de los proyectos de TI				X
ADECUACION				
Identificación de las soluciones automatizadas			X	
Adquisición y mantenimiento del software aplicativo			X	
Adquisición y mantenimiento de la infraestructura tecnológica			X	
Facilitad de operación y uso de TI		X		
Adquisición de recursos de TI		X		
Administración de cambios en TI			X	
Instalación y acreditación de soluciones y cambios en TI			X	
FORMALIZACION				
Definición y administración de los niveles de servicio			X	
Administración de los servicios de terceros			X	
Administración del desempeño y capacidad de TI			X	
Garantías en la continuidad del servicio			X	
Garantías en la seguridad de los sistemas			X	
Identificación y asignación de costos de TI			X	
Educación y entrenamiento a los usuarios			X	
Administración de la mesa de servicios de TI y los incidentes			X	
Administración de la configuración de TI			X	
Administración de los problemas con TI			X	
Administración de los datos			X	
Administración del ambiente físico		X		
Administración de las operaciones de TI		X		
DESARROLLO				
Monitoreo y evaluación del desempeño de TI		X		
Monitoreo y evaluación el control interno			X	
Garantías en el cumplimiento regulatorio			X	

Proporciona gobierno de TI			X	

ANEXO 05

BASE DE DATOS DE LA VARIABLE SEGURIDAD DE LA INFORMACIÓN

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
CONFIABILIDAD				
Control de las actividades de los equipo de computación	X			
Control del uso de los equipos	X			
Cambios, modificaciones o nuevo software cuentan con autorización de la gerencia	X			
Usuarios cuentan con una especificación sobre los programas que pueden acceder según sea su cargo dentro de la empresa		X		
Políticas frente a la propiedad intelectual y derechos de autor en la implantación y uso de software en la empresa				
INTEGRIDAD				
Se solicita a usuarios la respectiva autenticación en la red inalámbrica	X			
La red esta provista de FIREWALL adicional al incorporado en los sistemas operativos a fin de detectar y neutralizar la presencia de intrusos o hackers en la red	X			
Se lleva un registro de los mensajes lógicos de transmisión los cuales has de constar el origen, fecha, hora y receptor		X		
Se efectúa un registro aleatorio de las actividades de los usuarios de la red a fin de determinar los hábitos frecuentes de los mismos y detectar supuestas colaboraciones con terceros en el robo de información	X			
DISPONIBILIDAD				
Planificación adecuada para el mantenimiento de los equipos	X			
Manual de procedimientos de mantenimiento del hardware	X			
Sistemas operativos aplicaciones y paquetes utilitarios cuentan con licencia original	X			
Las fallas en los programas son documentadas y revisadas adecuadamente		X		
Existencia de programas actualizados de antivirus con el fin de evitar que los computadores presenten deficiencias en su funcionamiento lógico		X		
Se propone un proceso de evaluación previo al sistema para de esta manera poder interactuar mejor con el sistema principal		X		
Se indica un test a usuarios para promover mejor la utilización del software de la empresa	X			

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
CONFIABILIDAD				
Control de las actividades de los equipo de computación	X			
Control del uso de los equipos	X			
Cambios, modificaciones o nuevo software cuentan con autorización de la gerencia	X			
Usuarios cuentan con una especificación sobre los programas que pueden acceder según sea su cargo dentro de la empresa		X		
Políticas frente a la propiedad intelectual y derechos de autor en la implantación y uso de software en la empresa				
INTEGRIDAD				
Se solicita a usuarios la respectiva autenticación en la red inalámbrica	X			
La red esta provista de FIREWALL adicional al incorporado en los sistemas operativos a fin de detectar y neutralizar la presencia de intrusos o hackers en la red	X			
Se lleva un registro de los mensajes lógicos de transmisión los cuales has de constar el origen, fecha, hora y receptor	X			
Se efectúa un registro aleatorio de las actividades de los usuarios de la red a fin de determinar los hábitos frecuentes de los mismos y detectar supuestas colaboraciones con terceros en el robo de información	X			
DISPONIBILIDAD				
Planificación adecuada para el mantenimiento de los equipos	X			
Manual de procedimientos de mantenimiento del hardware	X			
Sistemas operativos aplicaciones y paquetes utilitarios cuentan con licencia original	X			
Las fallas en los programas son documentadas y revisadas adecuadamente	X			
Existencia de programas actualizados de antivirus con el fin de evitar que los computadores presenten deficiencias en su funcionamiento lógico	X			
Se propone un proceso de evaluación previo al sistema para de esta manera poder interactuar mejor con el sistema principal	X			
Se indica un test a usuarios para promover mejor la utilización del software de la empresa	X			

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
CONFIABILIDAD				
Control de las actividades de los equipo de computación	X			
Control del uso de los equipos	X			
Cambios, modificaciones o nuevo software cuentan con autorización de la gerencia	X			
Usuarios cuentan con una especificación sobre los programas que pueden acceder según sea su cargo dentro de la empresa		X		
Políticas frente a la propiedad intelectual y derechos de autor en la implantación y uso de software en la empresa				
INTEGRIDAD				
Se solicita a usuarios la respectiva autenticación en la red inalámbrica	X			
La red esta provista de FIREWALL adicional al incorporado en los sistemas operativos a fin de detectar y neutralizar la presencia de intrusos o hackers en la red	X			
Se lleva un registro de los mensajes lógicos de transmisión los cuales has de constar el origen, fecha, hora y receptor		X		
Se efectúa un registro aleatorio de las actividades de los usuarios de la red a fin de determinar los hábitos frecuentes de los mismos y detectar supuestas colaboraciones con terceros en el robo de información	X			
DISPONIBILIDAD				
Planificación adecuada para el mantenimiento de los equipos		X		
Manual de procedimientos de mantenimiento del hardware		X		
Sistemas operativos aplicaciones y paquetes utilitarios cuentan con licencia original		X		
Las fallas en los programas son documentadas y revisadas adecuadamente		X		
Existencia de programas actualizados de antivirus con el fin de evitar que los computadores presenten deficiencias en su funcionamiento lógico		X		
Se propone un proceso de evaluación previo al sistema para de esta manera poder interactuar mejor con el sistema principal	X			
Se indica un test a usuarios para promover mejor la utilización del software de la empresa		X		

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
CONFIABILIDAD				
Control de las actividades de los equipo de computación	X			
Control del uso de los equipos	X			
Cambios, modificaciones o nuevo software cuentan con autorización de la gerencia	X			
Usuarios cuentan con una especificación sobre los programas que pueden acceder según sea su cargo dentro de la empresa		X		
Políticas frente a la propiedad intelectual y derechos de autor en la implantación y uso de software en la empresa				
INTEGRIDAD				
Se solicita a usuarios la respectiva autenticación en la red inalámbrica		X		
La red esta provista de FIREWALL adicional al incorporado en los sistemas operativos a fin de detectar y neutralizar la presencia de intrusos o hackers en la red		X		
Se lleva un registro de los mensajes lógicos de transmisión los cuales has de constar el origen, fecha, hora y receptor		X		
Se efectúa un registro aleatorio de las actividades de los usuarios de la red a fin de determinar los hábitos frecuentes de los mismos y detectar supuestas colaboraciones con terceros en el robo de información		X		
DISPONIBILIDAD				
Planificación adecuada para el mantenimiento de los equipos		X		
Manual de procedimientos de mantenimiento del hardware		X		
Sistemas operativos aplicaciones y paquetes utilitarios cuentan con licencia original		X		
Las fallas en los programas son documentadas y revisadas adecuadamente		X		
Existencia de programas actualizados de antivirus con el fin de evitar que los computadores presenten deficiencias en su funcionamiento lógico		X		
Se propone un proceso de evaluación previo al sistema para de esta manera poder interactuar mejor con el sistema principal		X		
Se indica un test a usuarios para promover mejor la utilización del software de la empresa		X		

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
CONFIABILIDAD				
Control de las actividades de los equipo de computación		X		
Control del uso de los equipos		X		
Cambios, modificaciones o nuevo software cuentan con autorización de la gerencia		X		
Usuarios cuentan con una especificación sobre los programas que pueden acceder según sea su cargo dentro de la empresa		X		
Políticas frente a la propiedad intelectual y derechos de autor en la implantación y uso de software en la empresa		X		
INTEGRIDAD				
Se solicita a usuarios la respectiva autenticación en la red inalámbrica		X		
La red esta provista de FIREWALL adicional al incorporado en los sistemas operativos a fin de detectar y neutralizar la presencia de intrusos o hackers en la red		X		
Se lleva un registro de los mensajes lógicos de transmisión los cuales has de constar el origen, fecha, hora y receptor			X	
Se efectúa un registro aleatorio de las actividades de los usuarios de la red a fin de determinar los hábitos frecuentes de los mismos y detectar supuestas colaboraciones con terceros en el robo de información		X		
DISPONIBILIDAD				
Planificación adecuada para el mantenimiento de los equipos		X		
Manual de procedimientos de mantenimiento del hardware		X		
Sistemas operativos aplicaciones y paquetes utilitarios cuentan con licencia original			X	
Las fallas en los programas son documentadas y revisadas adecuadamente			X	
Existencia de programas actualizados de antivirus con el fin de evitar que los computadores presenten deficiencias en su funcionamiento lógico		X		
Se propone un proceso de evaluación previo al sistema para de esta manera poder interactuar mejor con el sistema principal		X		
Se indica un test a usuarios para promover mejor la utilización del software de la empresa		X		

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
CONFIABILIDAD				
Control de las actividades de los equipo de computación		X		
Control del uso de los equipos	X			
Cambios, modificaciones o nuevo software cuentan con autorización de la gerencia	X			
Usuarios cuentan con una especificación sobre los programas que pueden acceder según sea su cargo dentro de la empresa		X		
Políticas frente a la propiedad intelectual y derechos de autor en la implantación y uso de software en la empresa		X		
INTEGRIDAD				
Se solicita a usuarios la respectiva autenticación en la red inalámbrica		X		
La red esta provista de FIREWALL adicional al incorporado en los sistemas operativos a fin de detectar y neutralizar la presencia de intrusos o hackers en la red		X		
Se lleva un registro de los mensajes lógicos de transmisión los cuales has de constar el origen, fecha, hora y receptor		X		
Se efectúa un registro aleatorio de las actividades de los usuarios de la red a fin de determinar los hábitos frecuentes de los mismos y detectar supuestas colaboraciones con terceros en el robo de información			X	
DISPONIBILIDAD				
Planificación adecuada para el mantenimiento de los equipos		X		
Manual de procedimientos de mantenimiento del hardware			X	
Sistemas operativos aplicaciones y paquetes utilitarios cuentan con licencia original		X		
Las fallas en los programas son documentadas y revisadas adecuadamente			X	
Existencia de programas actualizados de antivirus con el fin de evitar que los computadores presenten deficiencias en su funcionamiento lógico		X		
Se propone un proceso de evaluación previo al sistema para de esta manera poder interactuar mejor con el sistema principal		X		
Se indica un test a usuarios para promover mejor la utilización del software de la empresa		X		

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
CONFIABILIDAD				
Control de las actividades de los equipo de computación		X		
Control del uso de los equipos		X		
Cambios, modificaciones o nuevo software cuentan con autorización de la gerencia	X			
Usuarios cuentan con una especificación sobre los programas que pueden acceder según sea su cargo dentro de la empresa		X		
Políticas frente a la propiedad intelectual y derechos de autor en la implantación y uso de software en la empresa		X		
INTEGRIDAD				
Se solicita a usuarios la respectiva autenticación en la red inalámbrica		X		
La red esta provista de FIREWALL adicional al incorporado en los sistemas operativos a fin de detectar y neutralizar la presencia de intrusos o hackers en la red		X		
Se lleva un registro de los mensajes lógicos de transmisión los cuales has de constar el origen, fecha, hora y receptor	X			
Se efectúa un registro aleatorio de las actividades de los usuarios de la red a fin de determinar los hábitos frecuentes de los mismos y detectar supuestas colaboraciones con terceros en el robo de información		X		
DISPONIBILIDAD				
Planificación adecuada para el mantenimiento de los equipos			X	
Manual de procedimientos de mantenimiento del hardware			X	
Sistemas operativos aplicaciones y paquetes utilitarios cuentan con licencia original			X	
Las fallas en los programas son documentadas y revisadas adecuadamente			X	
Existencia de programas actualizados de antivirus con el fin de evitar que los computadores presenten deficiencias en su funcionamiento lógico			X	
Se propone un proceso de evaluación previo al sistema para de esta manera poder interactuar mejor con el sistema principal			X	
Se indica un test a usuarios para promover mejor la utilización del software de la empresa			X	

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
CONFIABILIDAD				
Control de las actividades de los equipo de computación			X	
Control del uso de los equipos			X	
Cambios, modificaciones o nuevo software cuentan con autorización de la gerencia			X	
Usuarios cuentan con una especificación sobre los programas que pueden acceder según sea su cargo dentro de la empresa		X		
Políticas frente a la propiedad intelectual y derechos de autor en la implantación y uso de software en la empresa			X	
INTEGRIDAD				
Se solicita a usuarios la respectiva autenticación en la red inalámbrica			X	
La red esta provista de FIREWALL adicional al incorporado en los sistemas operativos a fin de detectar y neutralizar la presencia de intrusos o hackers en la red			X	
Se lleva un registro de los mensajes lógicos de transmisión los cuales has de constar el origen, fecha, hora y receptor			X	
Se efectúa un registro aleatorio de las actividades de los usuarios de la red a fin de determinar los hábitos frecuentes de los mismos y detectar supuestas colaboraciones con terceros en el robo de información			X	
DISPONIBILIDAD				
Planificación adecuada para el mantenimiento de los equipos			X	
Manual de procedimientos de mantenimiento del hardware				X
Sistemas operativos aplicaciones y paquetes utilitarios cuentan con licencia original			X	
Las fallas en los programas son documentadas y revisadas adecuadamente			X	
Existencia de programas actualizados de antivirus con el fin de evitar que los computadores presenten deficiencias en su funcionamiento lógico			X	
Se propone un proceso de evaluación previo al sistema para de esta manera poder interactuar mejor con el sistema principal			X	
Se indica un test a usuarios para promover mejor la utilización del software de la empresa			X	

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
CONFIABILIDAD				
Control de las actividades de los equipo de computación			X	
Control del uso de los equipos			X	
Cambios, modificaciones o nuevo software cuentan con autorización de la gerencia		X		
Usuarios cuentan con una especificación sobre los programas que pueden acceder según sea su cargo dentro de la empresa			X	
Políticas frente a la propiedad intelectual y derechos de autor en la implantación y uso de software en la empresa			X	
INTEGRIDAD				
Se solicita a usuarios la respectiva autenticación en la red inalámbrica			X	
La red esta provista de FIREWALL adicional al incorporado en los sistemas operativos a fin de detectar y neutralizar la presencia de intrusos o hackers en la red			X	
Se lleva un registro de los mensajes lógicos de transmisión los cuales has de constar el origen, fecha, hora y receptor			X	
Se efectúa un registro aleatorio de las actividades de los usuarios de la red a fin de determinar los hábitos frecuentes de los mismos y detectar supuestas colaboraciones con terceros en el robo de información		X		
DISPONIBILIDAD				
Planificación adecuada para el mantenimiento de los equipos				X
Manual de procedimientos de mantenimiento del hardware				X
Sistemas operativos aplicaciones y paquetes utilitarios cuentan con licencia original		X		
Las fallas en los programas son documentadas y revisadas adecuadamente			X	
Existencia de programas actualizados de antivirus con el fin de evitar que los computadores presenten deficiencias en su funcionamiento lógico			X	
Se propone un proceso de evaluación previo al sistema para de esta manera poder interactuar mejor con el sistema principal			X	
Se indica un test a usuarios para promover mejor la utilización del software de la empresa			X	

DIMENSIONES	ESCALAS			
	NO APLICA	CASI SE APLICA	APLICA REGULARMENTE	APLICA
CONFIABILIDAD				
Control de las actividades de los equipo de computación			X	
Control del uso de los equipos			X	
Cambios, modificaciones o nuevo software cuentan con autorización de la gerencia			X	
Usuarios cuentan con una especificación sobre los programas que pueden acceder según sea su cargo dentro de la empresa			X	
Políticas frente a la propiedad intelectual y derechos de autor en la implantación y uso de software en la empresa		X		
INTEGRIDAD				
Se solicita a usuarios la respectiva autenticación en la red inalámbrica			X	
La red esta provista de FIREWALL adicional al incorporado en los sistemas operativos a fin de detectar y neutralizar la presencia de intrusos o hackers en la red			X	
Se lleva un registro de los mensajes lógicos de transmisión los cuales has de constar el origen, fecha, hora y receptor			X	
Se efectúa un registro aleatorio de las actividades de los usuarios de la red a fin de determinar los hábitos frecuentes de los mismos y detectar supuestas colaboraciones con terceros en el robo de información		X		
DISPONIBILIDAD				
Planificación adecuada para el mantenimiento de los equipos	X			
Manual de procedimientos de mantenimiento del hardware	X			
Sistemas operativos aplicaciones y paquetes utilitarios cuentan con licencia original	X			
Las fallas en los programas son documentadas y revisadas adecuadamente		X		
Existencia de programas actualizados de antivirus con el fin de evitar que los computadores presenten deficiencias en su funcionamiento lógico		X		
Se propone un proceso de evaluación previo al sistema para de esta manera poder interactuar mejor con el sistema principal		X		
Se indica un test a usuarios para promover mejor la utilización del software de la empresa	X			

ANEXO 06

VALIDACIÓN DE JUICIO DE EXPERTO PARA EL CUESTIONARIO QUE MIDE LA VARIABLE AUDITORIA INFORMATICA

UNIVERSIDAD PRIVADA DEL NORTE

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE AUDITORIA INFORMATICA

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	PRELIMINAR	Si	No	Si	No	Si	No	
1	Definición del plan estratégico de TI	✓		✓		✓		
2	Definición de la arquitectura de la información	✓		✓		✓		
3	Determinación de la dirección tecnológica.	✓		✓		✓		
4	Definición de los procesos, organización y relaciones de TI.	✓		✓		✓		
	JUSTIFICACION	Si	No	Si	No	Si	No	
5	Administración de la inversión en TI	✓		✓		✓		
6	Comunicación con la Alta Dirección	✓		✓		✓		
7	Administración de los recursos humanos de TI.	✓		✓		✓		
8	Administración de la calidad de TI	✓		✓		✓		
9	Evaluación y administración de los riesgos de TI.	✓		✓		✓		
10	Administración de los proyectos de TI	✓		✓		✓		
	ADECUACION	Si	No	Si	No	Si	No	
11	Identificación de las soluciones automatizadas	✓		✓		✓		
12	Adquisición y mantenimiento del software aplicativo	✓		✓		✓		
13	Adquisición y mantenimiento de la infraestructura tecnológica	✓		✓		✓		
14	Facilitad de operación y uso de TI	✓		✓		✓		
15	Adquisición de recursos de TI	✓		✓		✓		
16	Administración de cambios en TI	✓		✓		✓		
17	Instalación y acreditación de soluciones y cambios en TI	✓		✓		✓		
	FORMALIZACION	✓		✓		✓		
18	Definición y administración de los niveles de servicio	✓		✓		✓		
19	Administración de los servicios de terceros	✓		✓		✓		
20	Administración del desempeño y capacidad de TI	✓		✓		✓		
21	Garantías en la continuidad del servicio	✓		✓		✓		
22	Garantías en la seguridad de los sistemas	✓		✓		✓		
23	Identificación y asignación de costos de TI	✓		✓		✓		
24	Educación y entrenamiento a los usuarios	✓		✓		✓		
25	Administración de la mesa de servicios de TI y los incidentes	✓		✓		✓		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: **Aplicable [✓]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: Mg: Corpus Aquino Jhon Jehyson **DNI:** 47051171

Especialidad del validador: Ing: Sistemas CIP: 173138

24 de Julio del 20.18

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

J&C CONSULTORA MULTISERVICIOS J&C
Ing. Corpus Aquino Jhon Jeh...
GERENTE GENERAL

Firma del Experto Informante.

UNIVERSIDAD PRIVADA DEL NORTE

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE AUDITORIA INFORMATICA

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	PRELIMINAR	Si	No	Si	No	Si	No	
1	Definición del plan estratégico de TI	✓		✓		✓		
2	Definición de la arquitectura de la información	✓		✓		✓		
3	Determinación de la dirección tecnológica.	✓		✓		✓		
4	Definición de los procesos, organización y relaciones de TI.	✓		✓		✓		
	JUSTIFICACION	Si	No	Si	No	Si	No	
5	Administración de la inversión en TI	✓		✓		✓		
6	Comunicación con la Alta Dirección	✓		✓		✓		
7	Administración de los recursos humanos de TI.	✓		✓		✓		
8	Administración de la calidad de TI	✓		✓		✓		
9	Evaluación y administración de los riesgos de TI.	✓		✓		✓		
10	Administración de los proyectos de TI	✓		✓		✓		
	ADECUACION	Si	No	Si	No	Si	No	
11	Identificación de las soluciones automatizadas	✓		✓		✓		
12	Adquisición y mantenimiento del software aplicativo	✓		✓		✓		
13	Adquisición y mantenimiento de la infraestructura tecnológica	✓		✓		✓		
14	Facilitad de operación y uso de TI	✓		✓		✓		
15	Adquisición de recursos de TI	✓		✓		✓		
16	Administración de cambios en TI	✓		✓		✓		
17	Instalación y acreditación de soluciones y cambios en TI	✓		✓		✓		
	FORMALIZACION							
18	Definición y administración de los niveles de servicio	✓		✓		✓		
19	Administración de los servicios de terceros	✓		✓		✓		
20	Administración del desempeño y capacidad de TI	✓		✓		✓		
21	Garantías en la continuidad del servicio	✓		✓		✓		
22	Garantías en la seguridad de los sistemas	✓		✓		✓		
23	Identificación y asignación de costos de TI	✓		✓		✓		
24	Educación y entrenamiento a los usuarios	✓		✓		✓		
25	Administración de la mesa de servicios de TI y los incidentes	✓		✓		✓		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: Aplicable [✓] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador. Mg.: MEJIA ARTEAGA MARION **DNI:** 32941575

Especialidad del validador: GESTION INTEGRAL DE RIESGOS

Matricula de colegiatura: 06-710

Chimbote 24 de Julio del 2018.

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

CAJA DEL SANTA S.A.
CPC Marion Mejia Arteaga

Firma del Experto Informante.

ANEXO 07

VALIDACIÓN DE JUICIO DE EXPERTO PARA EL CUESTIONARIO QUE MIDE LA VARIABLE SEGURIDAD DE LA INFORMACIÓN

UNIVERSIDAD PRIVADA DEL NORTE

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE SEGURIDAD DE LA INFORMACIÓN

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	CONFIABILIDAD	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	Control de las actividades de los equipo de computación	✓		✓		✓		
2	Control del uso de los equipos	✓		✓		✓		
3	Cambios, modificaciones o nuevo software cuentan con autorización de la gerencia	✓		✓		✓		
4	Usuarios cuentan con una especificación sobre los programas que pueden acceder según sea su cargo dentro de la empresa	✓		✓		✓		
5	Políticas frente a la propiedad intelectual y derechos de autor en la implantación y uso de software en la empresa	✓		✓		✓		
	INTEGRIDAD	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	Se solicita a usuarios la respectiva autenticación en la red inalámbrica	✓		✓		✓		
8	La red esta provista de FIREWALL adicional al incorporado en los sistemas operativos a fin de detectar y neutralizar la presencia de intrusos o hackers en la red	✓		✓		✓		
9	Se lleva un registro de los mensajes lógicos de transmisión los cuales has de constar el origen, fecha, hora y receptor	✓		✓		✓		
10	Se efectúa un registro aleatorio de las actividades de los usuarios de la red a fin de determinar los hábitos frecuentes de los mismos y detectar supuestas colaboraciones con terceros en el robo de información	✓		✓		✓		
	DISPONIBILIDAD	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	Planificación adecuada para el mantenimiento de los equipos	✓		✓		✓		
14	Manual de procedimientos de mantenimiento del hardware	✓		✓		✓		
15	Sistemas operativos aplicaciones y paquetes utilitarios cuentan con licencia original	✓		✓		✓		
17	Las fallas en los programas son documentadas y revisadas adecuadamente	✓		✓		✓		
18	Existencia de programas actualizados de antivirus con el fin de evitar que los computadores presenten deficiencias en su funcionamiento lógico	✓		✓		✓		
19	Se propone un proceso de evaluación previo al sistema para de esta manera poder interactuar mejor con el sistema principal	✓		✓		✓		
20	Se indica un test a usuarios para promover mejor la utilización del software de la empresa	✓		✓		✓		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: **Aplicable [✓]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: Mg. Corpus Aquino Jhon Jehyson **DNI:** 47051171

Especialidad del validador: Ing. Sistemas CIP: 173138

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

24 de Julio del 20.18.
J&C CONSULTORA-MULTISERVICIOS EIRL
J&C
Ing. Corpus Aquino Jhon Jehyson
GERENTE GENERAL

Firma del Experto Informante.

UNIVERSIDAD PRIVADA DEL NORTE

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE SEGURIDAD DE LA INFORMACION

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	CONFIABILIDAD	Si	No	Si	No	Si	No	
1	Control de las actividades de los equipo de computación	✓		✓		✓		
2	Control del uso de los equipos	✓		✓		✓		
3	Cambios, modificaciones o nuevo software cuentan con autorización de la gerencia	✓		✓		✓		
4	Usuarios cuentan con una especificación sobre los programas que pueden acceder según sea su cargo dentro de la empresa	✓		✓		✓		
5	Políticas frente a la propiedad intelectual y derechos de autor en la implantación y uso de software en la empresa	✓		✓		✓		
	INTEGRIDAD	Si	No	Si	No	Si	No	
7	Se solicita a usuarios la respectiva autenticación en la red inalámbrica	✓		✓		✓		
8	La red esta provista de FIREWALL adicional al incorporado en los sistemas operativos a fin de detectar y neutralizar la presencia de intrusos o hackers en la red	✓		✓		✓		
9	Se lleva un registro de los mensajes lógicos de transmisión los cuales has de constar el origen, fecha, hora y receptor	✓		✓		✓		
10	Se efectúa un registro aleatorio de las actividades de los usuarios de la red a fin de determinar los hábitos frecuentes de los mismos y detectar supuestas colaboraciones con terceros en el robo de información	✓		✓		✓		
	DISPONIBILIDAD	Si	No	Si	No	Si	No	
13	Planificación adecuada para el mantenimiento de los equipos	✓		✓		✓		
14	Manual de procedimientos de mantenimiento del hardware	✓		✓		✓		
15	Sistemas operativos aplicaciones y paquetes utilitarios cuentan con licencia original	✓		✓		✓		
17	Las fallas en los programas son documentadas y revisadas adecuadamente	✓		✓		✓		
18	Existencia de programas actualizados de antivirus con el fin de evitar que los computadores presenten deficiencias en su funcionamiento lógico	✓		✓		✓		
19	Se propone un proceso de evaluación previo al sistema para de esta manera poder interactuar mejor con el sistema principal	✓		✓		✓		
20	Se indica un test a usuarios para promover mejor la utilización del software de la empresa	✓		✓		✓		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: **Aplicable [✓]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Mg.: MESIA ARTEAGA MARLON **DNI:** 32941575

Especialidad del validador: GESTION INTEGRAL DE RIESGOS

Matricula de colegiatura: 06-710

[1]Pertinencia: El ítem corresponde al concepto teórico formulado.
[2]Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Chimbote 24 de Julio del 2018.

CAJA DEL SANTA S.A.
CPC. Marlon Mejia Arteaga
Firma del Experto Informante.

ANEXO 08

VALIDACIÓN ESTADISTICA PARA EL CUESTIONARIO QUE MIDE LA VARIABLE AUDITORIA INFORMATICA

CONFIABILIDAD

Confiabilidad por Alpha de Cronbach

Fórmula

$$\propto = \left[\frac{k}{k-1}\right]\left[1 - \frac{\sum_{i=1}^{k} S^2 i}{S_t^2}\right]$$

Donde

K: es el número de preguntas o Items

S^2_i: varianza del ítem

S^2_t : la varianza de los valores totales observados

K	11
∑Vi	6,1
Vt	23,6

SECCION 1	1,10
SECCION 2	0,74
ABSOLUTO	0,74

Alpha de Cronbach	0,8

ANEXO 09

VALIDACIÓN ESTADISTICA PARA EL CUESTIONARIO QUE MIDE LA VARIABLE SEGURIDAD DE LA INFORMACIÓN

CONFIABILIDAD

Confiabilidad por Alpha de Cronbach

Fórmula

$$\propto = \left[\frac{k}{k-1}\right]\left[1 - \frac{\sum_{i=1}^{k} S^2 i}{S_t^2}\right]$$

Donde

K: es el número de preguntas o Items

S^2_i: varianza del ítem

S^2_t : la varianza de los valores totales observados

K	11
∑Vi	7,1
Vt	21,3

SECCION 1	1,20
SECCION 2	0,71
ABSOLUTO	0,71

Alpha de Cronbach	0,8