UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

FACULTAD DE INGENIERÍA INDUSTRIAL, SISTEMAS E INFORMÁTICA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

PROPUESTA DE IMPLEMENTACION DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION BASADO EN LA NORMA ISO 27001 PARA UNA EMPRESA DE TELECOMUNICACIONES, 2021

Para optar el título profesional de Ingeniero de Sistemas

Presentado por el Bachiller:

FALCON FERNANDEZ, Junior Alejandro

Asesorado por:

Dr. ANGEL HUAMAN TENA

CIP No 41456

LIMA - HUACHO

2021

Tesis Falcon

INFORME DE ORIGINALIDAD

19%	13%	8%	14%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Cooperativa de Colombia Trabajo del estudiante	5%
2	ri.uaemex.mx Fuente de Internet	2%
3	Submitted to Universidad San Ignacio de Loyola Trabajo del estudiante	2%
4	Submitted to Universidad de Cádiz Trabajo del estudiante	1%
5	Submitted to Universidad Privada de Tacna Trabajo del estudiante	1%
6	rd.udb.edu.sv:8080 Fuente de Internet	1%
7	www.researchgate.net Fuente de Internet	1%
8	Submitted to Institución Tecnológica Metropolitana de Medellín Trabajo del estudiante	1%

MIEMBROS DEL JURADO Y ASESOR

……

PRESIDENTE

Ing.

……

SECRETARIO

Ing.

…….

VOCAL

Ing.

…….

ASESOR

Dr. Ángel Huamán Tena

DEDICATORIA

A Dios y mi Señor Jesús por su sabiduría.

A mis padres por ser guías

de cada acto que realizamos.

Autor

AGRADECIMIENTO

A mis familiares y amigos
Un especial agradecimiento por la
comprensión, paciencia y el ánimo recibido
Autor

PROPUESTA DE IMPLEMENTACION DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION BASADO EN LA NORMA ISO 27001 PARA UNA EMPRESA DE TELECOMUNICACIONES, 2021

PROPOSAL FOR THE IMPLEMENTATION OF AN INFORMATION SECURITY SYSTEM BASED ON THE ISO 27001 STANDARD FOR A TELECOMMUNICATIONS COMPANY, 2021

FALCON FERNANDEZ, Junior Alejandro[1]

RESUMEN

Objetivo: Determinar la influencia de la implementación de un Sistema de seguridad de la Información en la norma ISO 27001 para una empresa de telecomunicaciones**,** 2021.

Métodos: La siguiente investigación de tipo aplicada. El nivel de la investigación es Correlacional. La investigación tiene un diseño no experimental y transversal.

Resultados: Los resultados muestran que más del 80% de encuestados están de acuerdo con la propuesta de Implementar el Sistema de gestión de seguridad de la información basado en la norma ISO 27001 para una empresa de telecomunicaciones**,** 2021.

Conclusión: Existe una correlación positiva significativa moderada entre el modelo de inteligencia de negocio y la gestión administrativa (Rho = 0.697; p = 0.00 < 0.05).

Palabras claves: Sistema de seguridad de la información, norma ISO 27001 y Riesgo.

ABSTRAC

Objective: To determine the influence of the implementation of an Information Security System in the ISO 27001 standard for a telecommunications company, 2021.

Methods: The following applied type research. The level of investigation is Correlational. The research has a non-experimental and transversal design.

Results: The results show that more than 80% of respondents agree with the proposal to implement the information security system based on the standard iso 27001 for a telecommunications company, 2021.

Conclusion: There is a moderate significant positive correlation between the business intelligence model and administrative management (Rho = 0.697; p = 0.00 < 0.05).

Keywords: Information security system, ISO 27001 standard and Risk.

INDICE

II. MARCO TEORICO

III. METODOLOGIA

I. PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la realidad problemática

Ahora bien, las necesidades de las empresas están determinadas por el entorno global en el que viven, este entorno es muy competitivo; no hay duda de que existe una gran cantidad de empresas en todos los países y existe una gran competencia entre ellas; puede ser por productos, para mejorar sus recursos, para ingresar a nuevos mercados, entre otras cosas; requiere que las organizaciones se desempeñen bien para tener la oportunidad de competir con la enorme competencia que las rodea.

La promoción de nuevas tecnologías que conduzcan al desarrollo e integración de la SI dentro de una organización privada o pública para optimizar las operaciones y la gestión a través de una adecuada toma de decisiones. El uso de las nuevas tecnologías informáticas es un factor que contribuye al desarrollo de dichas habilidades (Flores, 2009). La gestión de la información es muy importante para la empresa ya que logra un alto nivel de competencia en el mercado y obtiene un mayor potencial de crecimiento. El propósito principal de la información es apoyar la toma de decisiones dentro de la organización; también pretende tener una base estable a partir de la cual decidir lo que se debe hacer y las direcciones en las que se lograrán los objetivos.

La información es un recurso equivalente a los recursos financieros, materiales y humanos que solían ser recursos de gestión de las empresas. Al analizar el surgimiento de las TI en las empresas, se destacan dos áreas importantes, como es la evolución del gobierno y las TI en las empresas. Actualmente, las empresas de telecomunicaciones no cuentan con un área o departamento de gestión de seguridad de la información, por lo que cada área de TI (Infraestructura, Telecomunicaciones, Desarrollo, etc.) seguridad de la información.

Tampoco tienen un SGSI documentado ni políticas de privacidad definidas o divulgadas. Algunas áreas tienen procesos pero no están centralizados y no se siguen de manera consistente. Por estas razones, es muy importante que estas empresas implementen el SGSI propuesto para fortalecer los controles que aseguren la disponibilidad, confidencialidad e integridad de su información. Y gestionar las amenazas a la seguridad de la información para mantenerlas en un nivel aceptable, teniendo en cuenta la clasificación de las amenazas y el auge del poder, desarrollo y uso racional de las tecnologías de la información y la comunicación en las empresas.

Por lo tanto, la propuesta de este proyecto es implementar de un sistema de gestion seguridad de la información basado en la norma ISO 27001 para una empresa de telecomunicaciones**,** 2021 con el propósito de mejorar sus mecanismos de control.

1.2 Formulación del problema

1.2.1 Problema general

¿De qué manera Influye la Implementación de un Sistema de seguridad de la Información basada en la norma ISO 27001 en una empresa de telecomunicaciones**,** 2021?

1.2.2 Problemas específicos

¿De qué manera Influye la Implementación de un Sistema de seguridad de la Información basada en la norma ISO 27001 en la Cantidad de Incidentes de Seguridad en una empresa de telecomunicaciones**,** 2021?

¿De qué manera Influye la Implementación de un Sistema de seguridad de la Información basada en la norma ISO 27001 en el Cumplimiento de nuevas normas establecidas para una empresa de telecomunicaciones**,** 2021?

¿De qué manera Influye la Implementación de un Sistema de seguridad de la Información basada en la norma ISO 27001 en el grado de satisfacción de los clientes con respecto al servicio que otorga una empresa de telecomunicaciones**,** 2021?

1.3 Objetivos

1.3.1 Objetivo general

Determinar la influencia de la implementación de un Sistema de seguridad de la Información basada en la norma ISO 27001 en una empresa de telecomunicaciones**,** 2021

1.3.2 Objetivos específicos

* Determinar la influencia de la Implementación de un Sistema de seguridad de la Información basada en la norma ISO 27001 en la Cantidad de Incidentes de seguridad en una empresa de telecomunicaciones**,** 2021
* Determinar la influencia de la Implementación de un Sistema de seguridad de la Información basada en la norma ISO 27001 en el Cumplimiento de nuevas normas establecidas para una empresa de telecomunicaciones**,** 2021
* Determinar la influencia de la Implementación de un Sistema de seguridad de la Información basada en la norma ISO 27001 en el grado de satisfacción de los clientes con respecto al servicio que otorga una empresa de telecomunicaciones**,** 2021

1.4 Justificación de la investigación

Para efectos de la investigación, los resultados permitieron realizar un estudio de vanguardia sobre el uso de los sistemas de seguridad de la información, revelando cómo un

adecuado análisis y diseño aseguran la calidad y cobertura oportuna de la información. También asegura que la información procesada sea confiable, a través de buenos controles informáticos internos y la tecnología utilizada en el proceso de desarrollo e implementación del proyecto, que los procedimientos estadísticos se lleven a cabo y que los procedimientos estadísticos sean transparentes y por ende la toma de decisiones Demostrado contribuir al proceso

1.5 Delimitación del estudio

1.5.1. Delimitación Espacial

Ciudad de Lima

1.5.2. Delimitación Temporal de la investigación

El periodo que comprende el estudio es 2021

1.5.3. Delimitación Social

El grupo social objeto de estudio del trabajo de investigación fueron el personal administrativo y técnico de la empresa de telecomunicaciones de la ciudad de Lima.

1.6 Viabilidad del estudio

1.6.1. Financiera

La investigación es propositiva porque se cree que no requiere altos costos económicos y corresponderá a la viabilidad financiera.

1.6.2. Acceso a la información

Una investigación es posible porque la información necesaria está fácilmente disponible y tenemos una gran cantidad de clientes descontentos en Lima y sus alrededores para que podamos obtener resultados.

CAPITULO II: MARCO TEORICO

2.1 Antecedentes de la investigación

2.1.1 Investigaciones Internacionales

Molano, R. (2017). *Estrategia para implementar un sistema de gestión de la seguridad de la información basada en la norma iso 27001 en el área de ti para la empresa market. MIX*. UNIVERSIDAD CATÓLICA DE COLOMBIA.

Objetivo:

Determinar la mejor estrategia para implementar un sistema de gestión de seguridad de TI basado en ISO 27001 para Market Mix.

Metodología:

ENFOQUE DE LA METODOLOGÍA Este estudio es de naturaleza mixta cualitativa y cuantitativa, ya que su propósito es recolectar datos a través de una encuesta cerrada y una entrevista abierta sobre la base de la observación, el análisis y la cuantificación, elaborado por el campo de los procesos de auditoría relacionados con la metodología de desarrollo de aplicaciones y sistemas de control de cambios dentro de la empresa.

TIPO DE ESTUDIO Este estudio es descriptivo porque permite la observación e interpretación de los resultados obtenidos mediante la recopilación de información a través de encuestas y entrevistas. Méndez (2003) afirma que “la investigación descriptiva utiliza criterios sistemáticos para revelar la estructura de los fenómenos estudiados y ayudar a establecer ciertos comportamientos mediante el control de métodos específicos de recopilación de datos. "

Conclusiones:

El propósito de este trabajo fue definir una estrategia para implementar un sistema de gestión de seguridad de la información para el sector TI de Market Mix luego de seleccionar herramientas que nos permitieran evaluar el estado actual de la región. TI, los datos recibidos han sido procesados y permiten determinar la mejor estrategia que debe desarrollarse paso a paso para lograr los objetivos establecidos. El uso estratégico y el seguimiento continuo de las tareas y responsabilidades asignadas a cada miembro permitirán identificar las amenazas a las que se enfrentan dentro de la organización, así como atacarlas y poner en marcha las medidas correctivas adecuadas para hacerlas más eficaces. mejorar y proteger continuamente la información para que la empresa no se vea afectada.

Tigse, J. (2020). *Plan de gestión de seguridad informática basado en la norma iso 27001 para el departamento de tecnología de la información en la empresa plasticaucho industrial S.A.* UNIVERSIDAD TÉCNICA DE AMBATO.

Objetivo:

Implementar un plan de gestión de seguridad informática basado en la Norma ISO 27001 para mejorar la seguridad de la información en la empresa plasticaucho industrial S.A

Metodología:

Modalidad Bibliográfica o Documental

Para mejorar la investigación se utilizarán estudios teóricos de diferentes autores, provenientes de fuentes de libros, artículos científicos, tesis de grado elaboradas en universidades, así como de otras fuentes documentos internos y externos de la empresa.

Modalidad de Campo

Se consideró este método porque la encuesta requería una visita de campo, donde el departamento de TI realizó controles de información para recopilar datos relacionados con los objetivos finales del trabajo. Se utilizarán los siguientes métodos: entrevistas, cuestionarios, observaciones e ISO 27001.

Conclusiones:

- Plasticaucho Industrial S.A. Actualmente cuenta con procedimientos de protección de la información definidos por el departamento de TI. En esta área se enrutan los procesos con base en políticas que permiten el control de las actividades del personal, software, hardware y recursos de información en general.
- La separación de tareas en el departamento de TI ha mejorado la calidad del servicio, donde cada miembro de la región identifica actividades de monitoreo y anomalías para aplicar procedimientos de resolución.
- Al contar con el Directorio Activo s posible identificar usuarios, equipos, tecnología y dispositivos de comunicación ubicados en el dominio corporativo y, mediante el uso de políticas de grupo, puede restringir el comportamiento al acceder a los recursos de la red
- Plasticaucho Industrial pudo reducir la responsabilidad por la integridad de los datos, la disponibilidad y las operaciones de seguridad a nivel de WAN mediante la subcontratación de servicios de red a proveedores externos, por lo que prestó más atención a la seguridad interna de la LAN. redes corporativas.

Gonzales, R. (2019). *Diseñar un modelo para implementar un sistema de gestión de seguridad de la información para una PYME del sector privado.* Universidad Católica de Colombia. Facultad de Ingeniería.

Objetivo:

Construyendo un modelo de implementación de un sistema de gestión de seguridad de la información para pequeñas y medianas empresas, es necesario garantizar la protección de la información no divulgada (confidencialidad), la información proporcionada debe ser precisa y completa desde la fuente desde la creación hasta la destrucción (integridad) y debe ser oportuna y en la forma requerida (disponibilidad) de acuerdo con las normas internacionales de seguridad.

Metodología:

Fases del trabajo de grado

El proyecto está diseñado en dos fases, la primera fase corresponde al diseño del modelo de implementación del SGSI, en el cual se examinará el contexto interno y externo que permita evidenciar la situación actual de seguridad de la información, luego se realizará el análisis de riesgos. determinación del nivel de gestión de riesgos (ARTE), SOA, GAP 27002. La segunda etapa implica que la empresa tome una decisión sobre la viabilidad consultiva de la próxima implementación con base en los resultados de la primera fase. sustentado en las actividades propuestas para desarrollar un modelo de SGSI que pueda ser implementado en este tipo de organizaciones.

Instrumentos o herramientas utilizadas Instrumentos:

Conocer el contexto interno de la organización a través de entrevistas de trabajo; revisar los procesos de negocio y las relaciones con la tecnología y la seguridad de la información; la prueba se realiza de manera razonable o informal de acuerdo con la norma internacional ISO 27001; análisis de la información representativa proporcionada por la empresa.

Conclusiones:

Para tener éxito en realizar el control de seguridad de la información en las pequeñas empresas, no hay algunas de sus actividades en el campo de la seguridad, la necesidad de comprender las necesidades y expectativas de las partes interesantes es el primer caso del primer caso. Tien. "Las partes interesadas pueden ser empleados de esta organización, accionistas, clientes, proveedores de bienes y servicios, proveedores de capital, asociaciones de víctimas o vecinos relacionados, sindicatos, otros sindicatos organizaciones civiles y estatales involucradas, etc." [Veintiún]. Luego, persuade y demuestre que sus necesidades y expectativas se pueden satisfacer con los requisitos de aplicación o control, lo que aumentará la seguridad en comparación con su propiedad, también especificando que las reglas y las reglas y las reglas de la aplicación para la industria (por ejemplo, se prescribe el sector educativo por el Ministerio de Educación y Finanzas del personal de gestión financiera y financiera de Colombia, etc. Según el número 1202 de un artículo de semana económica publicado en septiembre de 2019 [22], Asobancaria menciona, entre otras cosas, la responsabilidad de la alta dirección y el papel en la toma de decisiones estratégicas relacionadas con la gestión eficaz de los recursos de seguridad en su organización. incluye principios o recomendaciones sobre diez aspectos importantes de los cuales se destacan los siguientes:

Principio 5. Apetito de riesgo. La junta directiva debe identificar y cuantificar anualmente la tolerancia al riesgo de la empresa para la resiliencia cibernética y asegurarse de que se alinee con la estrategia y el apetito por el riesgo de la empresa.

Principio 6. Evaluación y reporte de riesgos. La junta debe facultar a la gerencia para realizar una evaluación cuantitativa y comprensible de los riesgos, amenazas e incidentes como un elemento regular en la agenda de sus reuniones

Principio 7. Planes de desarrollo sostenible. La gerencia debe asegurarse de apoyar a los empleados de resiliencia cibernética en el desarrollo, implementación, prueba y mejora continua de los planes de gestión de riesgos cibernéticos que sean apropiados para toda la organización. El oficial a cargo debe supervisar el trabajo e informar regularmente a la junta directiva.

Guardia, F. (2017). Diseño de un sistema de gestión de seguridad de la información ajustado a las necesidades de la corporación médica clínica vida de quibdó.

UNIVERSIDAD PONTIFICIA BOLIVARIANA ESCUELA INGENIERÍAS.

Objetivo:

Desarrollar un sistema de gestión de seguridad de la información acorde a las necesidades del grupo médico Clínica Vida de Quibdó para controlar mejor el riesgo de exposición a la información sobre la disponibilidad, integridad y autenticidad de la información contenida en las noticias.

Metodología:

Para desarrollar el proyecto del Sistema de Gestión de Seguridad de la Información, en línea con las necesidades del Grupo Médico Clínico Vida de Quibdó, se adoptaron como base los requisitos especificados por la norma NTCrISO/IEC 27001:2013 para la creación de un Sistema de Gestión, descritos a continuación y desarrollado en el capítulo 6: a) Definir el alcance y las limitaciones del SGSI en términos de negocio, organización, ubicación, tecnología y cualquier otra característica. b) Definir la política del SGSI en cuanto a las características de la empresa, su organización, su ubicación, activos y tecnología. c) Definir el enfoque de la organización para la evaluación de riesgos.

Conclusiones:

Al final de este proyecto, se descubrió que el sistema de gestión de seguridad de la información, desarrollado de acuerdo con las necesidades de la Clínica de Vida Quibdó, permite un mejor control de la información relacionada con la información sobre la capacidad de la capacidad de la capacidad. Uso, integridad y autenticidad de su información. Al desarrollar este proyecto, la situación actual de la Clínica de Vida se ha revelado en el campo de la gestión de la seguridad de la información, lo que permite el desarrollo de una propuesta para implementar el sistema de gestión de la información adecuado para la conclusión está en el diagnóstico, recibiendo todos los detalles necesarios en el campo de la infraestructura clínica para localizar y evaluar las amenazas y proteger la seguridad para construir un modelo basado en el modelo. El verdadero puente de la clínica. El modelo de seguridad de la información desarrollado en este trabajo requiere de constante actualización y retroalimentación, de lo contrario el modelo no estará totalmente alineado con futuras amenazas institucionales, ya que no crecerá con el crecimiento de la Clínica.

2.1.2 Investigaciones nacionales

Moscaiza, O (2018). *Diseño de un sistema de gestión de la seguridad de la información (SGSI) para la Cooperativa de Ahorro y Crédito ABC, basado en la norma ISO 27001:2013.* UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

Objetivo:

Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) para la Cooperativa de Ahorro y Crédito ABC, basado en la norma ISO 27001:2013, a fin

de gestionar los riesgos y garantizar un nivel adecuado de seguridad de la información

Metodología:

Esto es importante porque estas organizaciones necesitan crear valor para sus procesos comerciales. En primer lugar, 10 asociaciones de ahorro y crédito podrán lograr un aumento general en la eficacia de la seguridad de la información, ya que la introducción de un sistema de gestión mejorará la gestión de los procesos comerciales. Segundo, las cooperativas de ahorro y crédito podrán reducir sus costos. Esto se debe a la racionalización de los recursos y al correcto manejo de todos los riesgos que asumen.

Conclusiones:

La valoración de los activos de información en ABC Cooperativa de Ahorro y Crédito ABC permite a una entidad identificar lo que es importante desde el punto de vista de sus objetivos de negocio, ayudando a identificar quién es responsable de su gestión, así como la frecuencia y clasificación. De esta manera, podemos demostrar que CAC ha mejorado significativamente su gestión de activos en comparación con su estado original, asegurando así una gestión de riesgos efectiva.

b. El análisis de los procesos ayuda a identificar las principales amenazas a la seguridad de la información en la Cooperativa de Ahorro y Crédito Azbuka con mayor eficiencia que la línea de base. Teniendo esto en cuenta, podemos mostrar que la Cooperativa ha mejorado la gestión de riesgos del 22,22% original debido a que tiene un análisis bajo por la falta de una metodología determinista.

c. Este proyecto identificó procedimientos de gestión de riesgos de seguridad de la información para respaldar los procesos y objetivos comerciales mediante la selección de controles del Anexo A de la norma ISO 27001:2013, y analizó cómo

el mejor enfoque para abordar cualquier riesgo e impacto potencial depende de la gravedad o la sensibilidad del recurso.

d. Se han desarrollado directrices para establecer un nivel inicial de requisitos de ISO 27001:2013 y un nivel de madurez de control, lo que da como resultado un punto final de cumplimiento del 15 % para los requisitos de los capítulos del reglamento y del 25 % para los controles del Anexo A. Esto mejorará cada momento en que se implementen las acciones de mejora identificadas en el Plan Estratégico de Seguridad de la Información.

e. La validación de este modelo de sistema de gestión de seguridad de la información permite la elaboración de un Plan Estratégico de Seguridad de la Información CAC debido a la unificación de los resultados de ISO 27001:2013, ISO 27002:2013 dominio alcance y resultados analizar la diferencia. En base a los valores obtenidos, se pueden determinar los planes de seguridad adecuados.

Castillo, R. (2016). *Sistema de gestión de seguridad de la información en la municipalidad distrital de pira aplicando la norma iso/iec 27001:2013.* Universidad Católica Los Ángeles.

Objetivo:

Analizar, diseñar, desarrollar e implementar un sistema informático para el control, seguimiento y mantenimiento de los equipos hospitalarios del Hospital Central de la Fuerza Aérea del Perú.

Metodología:

Esta tesis es un estudio Cuantitativa porque se describen, analizan o prueban las variables de investigación.

De acuerdo con la hora del incidente, la investigación será RETROSPECTIVA a medida que se recuperan los registros de datos del departamento de programación y auditoría del departamento de ingeniería de HCFAP

De acuerdo con el análisis y alcance de los hallazgos, el estudio se realizará como parte de un estudio DESCRIPTIVA ya que tiene como objetivo identificar características importantes, significativas o distintas del sujeto de investigación, muestra o población a observar.

Conclusiones:

• El mantenimiento es ahora considerado un elemento estratégico, por lo que el Hospital Central FAP siempre se esfuerza por aumentar su competitividad y eficiencia implementando métodos y sistemas que permitan sistematizar y actualizar gran cantidad de información para una gestión eficaz.

• El uso de un programa preventivo y/o de reparación tiene un impacto directo en el aprovechamiento óptimo de la vida útil de los equipos, la continuidad de los procesos y el logro de los más altos niveles de seguridad y confiabilidad, y así reducir los costos de operación.

• Las herramientas del sistema informático son útiles para monitorear y programar actividades y mantener el historial de cada dispositivo. Con la información recopilada se puede obtener una variedad de resultados e indicadores para evaluar la gestión del mantenimiento.

• La implementación del sistema de información para planificar el mantenimiento de las obras, así como el control del control de inventario del equipo hospitalario, mejorará la gestión del inventario y luego la ventaja del trabajo aumentó el cumplimiento de la accesibilidad del dispositivo.

• El sistema permitirá que las piezas y partes del hospital FAP administren sus aplicaciones para pedidos directamente a través del sistema, de esta manera se acelerará y reducirá la reserva y reserva y le permitirá controlar mejor un estado en el que se puede encontrar en el que se puede encontrar en el que se puede encontrar en el que se puede encontrar en el que se puede encontrar en el que se puede encontrar El trabajo de pedidos creado por los usuarios.

Bendezú N. (2014). *"Implementación de un sistema de información basado en un enfoque de procesos, para la mejora de la operatividad del área de créditos de la microfinanciera CRECER".* Universidad Nacional del Centro del Perú.

Objetivo:

Determinar el impacto de la implementación de un Sistema de Información Basado en Procesos en la operación del sector microfinanciero CRECER.

Metodología:

Este estudio es de carácter aplicado ya que muestra la aplicación de conocimientos teóricos en el campo de la gestión de procesos y sistemas de TI para cambiar procesos y crear software especial para obtener los resultados deseados para mejorar el trabajo del sector crediticio de Microfinanzas CRECER.

Conclusiones:

1. Gracias a la aplicación e implementación del sistema informático COREBANK en la microfinanciera CRECER, se ha mejorado el área de crédito de la entidad designada, reduciendo la tasa de morosidad en 0.83%, equivalente a S/. 25.000 soles, acortando el tiempo de revisión de crédito en 20,6 horas, mejorando la satisfacción del cliente en 1,1 puntos y la satisfacción de los empleados en 1,1 puntos.

2. a implementación de un sistema informático basado en un enfoque de procesos ayuda a resolver y manejar cada proceso que se lleva a cabo en el departamento de crédito de la empresa de microfinanzas CRECER.

3. Implementar las mejores prácticas recomendadas por el método XP en las etapas de desarrollo del software nos permite desarrollar todos los requisitos funcionales y cumplir con precisión las fechas de entrega en cada iteración.

4. La arquitectura jerárquica proporciona una mejor escalabilidad para futuras integraciones con nuevas herramientas y servicios mediante la reutilización de componentes.

5. A través de la implementación del Sistema de TI COREBANK, que está diseñado para acompañar la corrección de cada proceso, es posible incentivar e implementar estas mejores prácticas entre los empleados de la organización y aumentar su eficacia.

Saldoval, A. (2019). *Sistemas de información estratégicos para la toma de decisiones de un contact center en lima moderna, AÑO – 2018*. Universidad San Ignacio de Loyola.

Objetivo:

Rediseñar el sistema estratégico de TI del centro de contacto para agilizar de manera eficiente y eficaz el proceso de toma de decisiones de gestión.

Metodología:

Nuestro argumento es bidireccional porque utilizaremos dos variables: los sistemas de información estratégica y la toma de decisiones; cuantitativa, ya que ambas variables representan datos numéricos en sus índices; correlación, porque se utilizará estadística inferencial para mostrar la relación entre ambas variables;

y el modelo positivista porque creemos que beneficiará a la humanidad. Nuestra tesis de grado es una investigación, por el tipo de construcción que llamaremos cuasi experimental porque estaremos trabajando con muestreo - porque los datos son predeterminados, no aleatorios. El tipo de estudio fue transversal en el tiempo porque el estudio se limitó a 2018 para medir o caracterizar la situación en ese momento en particular.

Conclusiones:

La modernización integral de los sistemas estratégicos de TI (ERP, BI, CRM, WFM) es posible de forma independiente gracias a los datos que posee el centro de contacto en Lima Moderna y se integran como fuente de información, datos de entrada de datos para muchos empleados en puestos de alto nivel. . La modernización integral de los sistemas de información estratégica (ERP, BI, CRM, WFM) garantiza en gran medida la interoperabilidad del centro de contacto en Lima moderna entre los gerentes de toma de decisiones con los subordinados y las carteras de sus clientes. Esto se ha logrado a través de informes automatizados que tienen un impacto más positivo en beneficio de usted, sus empleados y sus clientes. La modernización integral de los sistemas estratégicos de TI (ERP, BI, CRM, WFM) en un moderno centro de contacto de Lima garantiza un fácil acceso y uso de datos críticos que contribuyen al análisis, así como una forma de integrar datos corporativos con procesos de ejecución de decisiones en todo el centro de contacto de la pirámide de la organización. Gracias a la modernización integral de la decisión tomada, contactar en la Lima contemporánea ha permitido que la decisión diaria se incline, de hecho, se han confiado diferentes autores, desde el pago hasta la administración (con énfasis en los resultados correctos, alcanzar los objetivos, aumentar los costos. , obtener

resultados, obtener resultados) y efectividad (con 121 presión en los medios, los principales cadáveres de casos, resolución de problemas, ahorro de costos, finalización de tareas y obligaciones); Por lo tanto, asegúrese de que en cada relación en la que se tome el proceso de tomar la decisión, solo tiene acceso a la información necesaria para resolver todos los tipos de habilidades específicas y, por lo tanto, es posible lograr la distribución de información en toda la pirámide organizada. El centro de contacto dentro de los límites modernos requiere que las herramientas contribuyan rápidamente a los cambios constantes que requieren el mercado actual y gracias a la ayuda de la modernización integrada con sistemas de TI estratégicos (ERP, BI, CRM, WFM), se pueden mejorar y puede mantenerse en Frente a una organización de manera más efectiva, de manera más efectiva, más eficiente, mayor eficiencia y competencia para desarrollar nuevas estrategias de mercado y, seguramente bloquear, mejorar sus resultados.

2.2 Bases teóricas

2.2.1 Sistema de seguridad de la información

2.2.1.1 Los sistemas de información en las organizaciones

Según Laudon y Laudon (2016), los sistemas de información se han convertido en herramientas comunes en línea, participando activamente en las actividades diarias y en la toma de decisiones en las organizaciones. El sistema de información se puede considerar como un factor de producción que puede reemplazar el capital y el trabajo. Los autores también señalan que los sistemas de información han reemplazado gradualmente los procedimientos manuales con procedimientos,

procesos y flujos de trabajo automatizados. Para WDFG Perú, cuando se convierta en emisor electrónico, algunos procesos manuales se realizarán de manera automática. Según David (2014), el proceso de gestión estratégica se simplifica significativamente si las empresas cuentan con un sistema de TI adecuado y eficaz. Un buen sistema informático permite a las empresas reducir costes. Al implementar la facturación electrónica en WDFG Perú, se reducirán los costos directos, indirectos y ocultos mencionados en capítulos anteriores.

Según Porter (2009), es muy importante comprender la estructura de las empresas o industrias ya que determinan la rentabilidad y la competencia. De igual forma, el autor muestra que la rentabilidad de la industria estará íntimamente relacionada con el poder dominante de la firma.

Porter (2009) propone cinco fuerzas: amenaza de nuevos competidores, poder de negociación de los proveedores, poder de negociación de los compradores, amenaza de sustitutos y competencia. En empresas o industrias competitivas que intentan mantenerse en el negocio, lo hacen mediante la introducción de productos o servicios innovadores que hacen el mejor uso de la tecnología y los sistemas. La información pertenecerá al grupo de empresas o industrias con la mayor ventaja competitiva.

Las empresas o industrias que están comprometidas con la satisfacción del cliente y buscan agregar valor a sus productos o servicios confían en los sistemas de información como una forma de negociar con los clientes, como por ejemplo a través de un sitio web que pueden visitar para recopilar información o hacer recomendaciones. . Otra fuerza es la amenaza de productos sustitutos, las empresas o industrias a menudo se ven amenazadas por productos o servicios que

funcionan igual o mejor, por lo que la innovación a través del sistema de información La confianza es necesaria para crear una ventaja competitiva.

2.2.1.2 Seguridad Informática

La seguridad informática asegura la integridad, disponibilidad y acceso a la información propiedad de la entidad, cuyo objetivo principal es mantener el mínimo riesgo a los recursos informáticos para asegurar la continuidad de las operaciones de la organización, reduciendo los costos administrativos, organizados de acuerdo con métodos de seguridad administrativa, también permite el almacenamiento de documentos, registros y archivos informáticos de las empresas, siempre completos y completamente confiables.

Las cuatro áreas principales que cubre la seguridad informática:

1. **Confidencialidad**: Sólo los usuarios autorizados pueden acceder a nuestros recursos, datos e información.
2. **Integridad**: Sólo los usuarios autorizados deben ser capaces de modificar los datos cuando sea necesario.
3. **Disponibilidad**: Los datos deben estar disponibles para los usuarios cuando sea necesario.
4. **Autenticación**: Estás realmente comunicándote con los que piensas que te estás comunicando.

La seguridad informática es importante para prevenir el robo de datos tales como números de cuentas bancarias, información de tarjetas de crédito, contraseñas, documentos, etc., que es algo esencial durante las comunicaciones de hoy en día

2.2.1.3 Amenazas a la Seguridad de la Información

Amenaza se refiere a cualquier tipo de elemento o actividad que tiene como objetivo crear una amenaza a la seguridad de la información, los mismos factores que surgen cuando se descubre una vulnerabilidad a la seguridad se pueden utilizar de muchas formas diferentes, ya sea daño o robo de información. Se presenta un aumento en el número de vulnerabilidades del lado del usuario debido al uso inadecuado de la tecnología, así como diversas técnicas como ingeniería social, falta de capacitación del personal y mayor rentabilidad de los ataques.

Para conseguir un sistema de información seguro y confiable se establecen una serie de estándares, protocolos, métodos, reglas y técnicas. Sin embargo, existen amenazas que deben tenerse en cuenta:

* **Usuarios**: Se considera la causa del mayor problema ligado a la seguridad de un sistema informático, es así porque con sus acciones podrían ocasionar graves consecuencias.

* **Programas maliciosos**: Conocidos como malware que son destinados a perjudicar un ordenador cuando se instala o hacer uso ilícito de datos.

* **Errores de programación**: Se trata de un mal desarrollo, pero también se tiene que ver como un riesgo evitando que los sistemas operativos y aplicaciones estén sin actualizar.

* **Intrusos**: Cuando personas que no están autorizadas acceden a programas o datos que no deberían.

* **Siniestro**: También se puede perder o deteriorar material informático por una mala manipulación o mala intención, tales situaciones como robo, incendio o inundación.

* **Fallos electrónicos**: Un sistema informático en general puede verse afectado

por problemas del suministro eléctrico o por errores lógicos como cualquier otro dispositivo que no es perfecto.

* **Catástrofes naturales**: Rayos, terremotos, inundaciones.

* **Copias de seguridad**: Para proteger de forma eficiente los datos son imprescindibles las copias de seguridad o backups.

2.2.1.4 Vulnerabilidades

Las vulnerabilidades de seguridad son vulnerabilidades obvias en los sistemas informáticos y donde operan; la presencia exclusiva de una o más vulnerabilidades en sí no es dañina, hace necesaria la amenaza de explotación y genera problemas en la organización empresarial, por lo que se puede concluir que si la vulnerabilidad no provoca que suponga ninguna amenaza no es necesario aplicar la verificación.

Las áreas que se pueden identificar vulnerabilidades son:

* **Organización**: es afectado por ser el lugar físico donde trabajan un conjunto de personas tanto internas como externas.

* **Procesos y procedimientos**: los procesos y procedimientos se verán afectados por su participación en el manejo de la información.

* **Personal**: es el principal responsable de que las vulnerabilidades afecten a la organización por ser el que trabaja y manipula la información sean físicos o lógicos.

* **Ambiente**: se verá afectado el ambiente cuando no se siga lineamientos para mantener un espacio estable y libre de amenazas.

* **Configuraciones de los sistemas de información**: al no existir una correcta configuración de los sistemas de información, se deja abierto una brecha para posibles vulnerabilidades que sean explotadas por personas mal intencionadas.

* **Hardware y Software**: el escoger el tipo de tecnología que se vaya a utilizar para las labores de la empresa, debe ser tomando en cuenta la seguridad que ofrece y los beneficios que se obtiene al utilizarlos.

* **Equipos de comunicación:** es importante considerar la seguridad de los medios de comunicación, ya que en una organización siempre se mantendrá interacción con varios usuarios internos y externos.

2.2.1.5 Administración de Riesgos

Un proceso interactivo e iterativo basado en el conocimiento, evaluación y gestión de los riesgos y sus consecuencias para mejorar la toma de decisiones en la organización. La gestión de riesgos se puede aplicar en cualquier situación que genere una oportunidad de mejora para la empresa, los principales factores que se deben tener en cuenta en el marco de TI son: seguridad, control (prevención, detección y remediación), lineamientos de uso y políticas. se implementan para evitar el impacto en el alcance de todas las actividades de la organización en sus planes comerciales, financieros, administrativos y sistémicos. La aplicación de la norma ISO 27001 en el campo de la seguridad y gestión de riesgos es una de las tareas más importantes cuando queremos identificar proyectos e iniciativas a través de los cuales pretendemos mejorar la seguridad de la información en su organización. El objetivo tras el análisis de riesgos es poder reducir el riesgo de la empresa a un nivel aceptable en base al análisis de la situación subyacente.

2.2.1.6 Plan de Gestión de Seguridad Informática

Un Plan de Gestión de la Seguridad de la Información es un conjunto de herramientas las medidas administrativas, técnicas y de personal están relacionadas

Garantizan un nivel de seguridad informática adecuado al peso de la mercancía protegida y al riesgo percibido. Un plan de gestión de la seguridad informática es el documento básico que define los principios organizativos y funcionales de las actividades de seguridad informática de una entidad y establece todas las políticas seguridad y responsabilidad de los involucrados en el proceso informático, así como medidas y procedimientos para prevenir, detectar y responder a las amenazas que lo agobian.

2.2.1.7 Sistemas de Gestión de la Seguridad de la Información (SGSI)

SGSI tiene un enfoque sistemático utilizado para gestionar la información confidencial de una organización empresarial con el fin de mantener su integridad y confidencialidad. Este modelo de gestión de riesgos incluye a todo el personal, procesos internos, procesos externos y sistemas gestionados por el departamento de TI. La implementación del SGSI ayuda a las pequeñas, medianas y grandes empresas

cuidar la confidencialidad de las fuentes de información, lo que permitirá a la empresa mejorar su reputación frente a sus competidores.

2.2.1.8 International Organization for Standardization (ISO)

SGSI tiene un enfoque sistemático utilizado para gestionar la información confidencial de una organización empresarial con el fin de mantener su integridad y confidencialidad. Este modelo de gestión de riesgos incluye a todo el personal, procesos internos, procesos externos y sistemas gestionados por el departamento de TI. La implementación del SGSI ayuda a las pequeñas, medianas y grandes empresas

cuidar la confidencialidad de las fuentes de información, lo que permitirá a la empresa mejorar su reputación frente a sus competidores.

2.2.2 ISO 27001

La Norma Estándar ISO 27001 tiene un enfoque sistemático utilizado para gestionar la información confidencial de una organización empresarial con el fin de mantener su integridad y confidencialidad. Este modelo de gestión de riesgos incluye a todo el personal, procesos internos, procesos externos y sistemas gestionados por el departamento de TI. La implementación la Norma Estándar ISO 27001 ayuda a las pequeñas, medianas y grandes empresas cuidar la confidencialidad de las fuentes de información, lo que permitirá a la empresa mejorar su reputación frente a sus competidores.

2.3 Bases filosóficas

El Código de Sistemas de Información (SI) está experimentando una crisis de identidad. Para abordarlo, algunos autores utilizan ideas de diferentes tradiciones filosóficas. Por otro lado, la PI y sus consecuencias son motivo necesario de reflexión en la filosofía contemporánea. Estos dos factores han contribuido a la convergencia de la disciplina y la filosofía de la propiedad intelectual y han creado un diálogo entre ellas. De esta manera, comenzó a surgir un campo que podría llamarse filosofía de la informática, en el que surgieron cuestiones ontológicas, epistemológicas, metodológicas, axiomáticas, filosóficas y surgió otra escuela tradicional. En esta conferencia, presento un programa de introducción a la filosofía de la informática. Intento explicar su naturaleza, cuáles son las amenazas, en qué herramientas intelectuales puede confiar y sugerir algunos núcleos temáticos clave. La filosofía de la informática debe ser también la filosofía de la informática. Entonces, la historia

debe ser un diálogo real, no solo una reflexión filosófica sobre el tema de otra persona. De hecho, la filosofía puede explicar la naturaleza y las consecuencias de la computación desde un punto de vista histórico y contemporáneo. Asimismo, puede involucrarse en el desarrollo de una visión compartida que refleje la relación de la informática con otros campos del conocimiento y la actividad humana. También puede contribuir a una discusión metodológica y aclarar conceptos clave (sistemas, información, modelos...).

2.4 Definiciones conceptuales

ACCESO: Es un permiso o conjunto de permisos otorgados a un usuario para acceder a los recursos informáticos de acuerdo con las responsabilidades asignadas y el cargo o actividad laboral.

ACTIVO O RECURSO DE INFORMACIÓN: Son todos los recursos de información y técnicos, activos tangibles e intangibles, necesarios o complementarios para el desarrollo de los objetivos empresariales, cualquiera que sea la presentación, medio o formato en que se creen, existan o utilicen.

ADMINISTRADOR DE LA INFORMACIÓN: La persona responsable de almacenar la información proporcionada por el Oficial de Información.

AUTENTICACIÓN: El proceso de verificar la identidad de un usuario, dispositivo o proceso que intenta acceder a un sistema.

AUTORIZACIÓN:

El proceso de concesión de privilegios para realizar acciones en el sistema.

CONFIDENCIALIDAD: Una propiedad que determina que la información no está disponible o divulgada a personas, organizaciones o procesos no autorizados.

DISPONIBILIDAD: La propiedad que determina quién puede acceder y utilizar la información cuando lo requiera un individuo, departamento o proceso autorizado.

ESTÁNDAR: Un conjunto de parámetros específicos para cada tecnología informática utilizada.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Cualquier situación asociada con el estado de un sistema de información, servicio de red o hardware que identifique o no identifique una posible violación de las políticas de seguridad de la información o un riesgo de falla de los controles implementados.

GESTION DE RIESGO: El proceso de gestión y control del riesgo.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Un evento o secuencia de eventos que amenaza la confidencialidad y/o integridad y/o disponibilidad de información y recursos técnicos de apoyo, poniendo en peligro la operación y seguridad de la UES.

INFORMACIÓN CONFIDENCIAL Y PRIVILEGIADA: Esta es toda la información de UES y cualquier divulgación no autorizada podría comprometer los planes, objetivos estratégicos y/o reputación de UES o comprometer la responsabilidad de UES ante terceros. El número de personas que tienen acceso a este tipo de información es limitado y debe ser estrictamente controlado.

INFORMACIÓN CRÍTICA: Toda la información considerada esencial para la ejecución de un proceso de negocio.

INFORMACIÓN DE USO INTERNO: Información de uso selectivo. Su acceso se basa en su necesidad de conocerlo o usarlo para realizar las funciones de un proceso UES o un rol específico.

INFORMACIÓN PUBLICA: Información dirigida al público. Su divulgación se hace a través de los canales institucionales establecidos por la UES.

INTEGRIDAD: Propiedad de salvaguardar la exactitud y estado completo de los activos de información.

RIESGO DE TI/INFORMACIÓN: Eventos potenciales relacionados con el uso de la tecnología y/o la información (física o electrónica), los cuales pueden ser explotados por amenazas debido a la presencia de vulnerabilidades, generando un impacto a los procesos de una UES.

SEGURIDAD DE LA INFORMACIÓN: Es el conjunto de medidas de protección que ejerce la UES contra divulgación o modificación no autorizada, hurto o destrucción accidental o intencionada de su información y de la información de terceros que está bajo su cuidado. Estas medidas de protección se basan en el valor relativo de la información y el riesgo en el que se pueda ver comprometida.

2.5 Formulación de la hipótesis

2.5.1 Hipótesis general

La Implementación de un Sistema de gestión de seguridad de la Información basado en la norma ISO 27001 influye en una empresa de telecomunicaciones**,** 2021

2.5.2 Hipótesis específicos

La Implementación de un Sistema de gestión de seguridad de la Información basado en la norma ISO 27001 Influye en la Cantidad de Incidentes de Seguridad en una empresa de telecomunicaciones**,** 2021

La Implementación de un Sistema de gestión de seguridad de la Información basado en la norma ISO 27001 Influye en el Cumplimiento de nuevas normas establecidas para una empresa de telecomunicaciones**,** 2021

La Implementación de un Sistema de gestión de seguridad de la Información basado en la norma ISO 27001 Influye en el grado de satisfacción de los clientes con respecto al servicio que otorga una empresa de telecomunicaciones, 2021

2.6 Operacionalización de Variables e Indicadores

Ver cuadro N° 01.

Cuadro N° 01

Operacionalización de Variables e Indicadores

Variables	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Instrumento
V.I.: Sistemas de Gestión de Seguridad de la Información	Conjunto formal de procesos que, operando con un conjunto de datos de acuerdo a las necesidades de una empresa, recopila, elabora y distribuye la información necesaria para la operación de dicha empresa y para las actividades de dirección, de control correspondientes (Andreu, Ricart y Valor, 1996)	La seguridad de la información en las empresas se considera que es un conjunto de responsabilidades, procesos, procedimientos y recursos que establece la alta dirección	Disponibilidad de la información	% de Reportes entregados en el plazo	*Cuestionario*
			Integridad de la información	% de Reportes Íntegros generados	*Cuestionario*
			Confidencialidad de la información	% de Reportes Confidenciales Entregados Correctamente	*Cuestionario*
V.D.: **Norma Iso 27001**	ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.		* Incidentes de Seguridad	* Cantidad de Incidentes de Seguridad	*Encuesta*
			*Cumplimiento de nuevas normas establecidas	* Cumplimiento de nuevas normas establecidas	*Encuesta*
			* Satisfacción de los clientes con respecto al servicio		

CAPITULO III: METODOLOGIA

La investigación realizada se basa en el método de análisis y síntesis, el estudio de casos y en el método general de solución de problemas aplicado a los sistemas de información.

3.1 Diseño Metodológico

Para llevar a cabo la investigación será de tipo documental, posteriormente aplicada y de campo. A continuación, se describen:

a) **Investigación documental**.

Se procederá a la búsqueda y recopilación de las fuentes de información, bibliográficas y multimedia bajo el siguiente esquema.

• Revisión de bibliografías, artículos y trabajos especiales sobre el tema.

• Lectura y revisión de investigaciones aplicadas en Sistemas de Información.

b) **Investigación aplicada**

Una vez concluida la investigación documental se realizarán las siguientes actividades:

• Visualización y análisis del material.

• Clasificación del material analizado de acuerdo con su importancia para el trabajo de investigación.

• Selección de elementos y temas fundamentales de acuerdo con la forma que incidan en el trabajo de investigación.

3.1.1 Tipo

Esta investigación es una investigación aplicada, lo que implica utilizar el conocimiento en la práctica para aplicarlo en la mayoría de los casos en beneficio de la empresa.

Estudios de grado de correlación, ya que su finalidad es establecer el grado de asociación o relación no causal entre dos o más variables. Se caracterizan porque las variables se miden primero, luego se estiman las correlaciones probando las hipótesis de correlación y aplicando métodos estadísticos.

3.1.2 Nivel de la Investigación

El nivel de la investigación es Correlacional, ya que se busca la relación entre las variables planteadas en la investigación Diseño de un sistema de información y el proceso de búsqueda de registro civil en la municipalidad distrital de Vegueta.

El método es deductivo ya que va de lo general a lo particular. Se comienza con la teoría, de la cual se derivan expresiones lógicas que se busca someter a prueba.

3.1.3 Diseño

El diseño de una investigación es la estrategia o plan utilizado para responder el problema de investigación; asimismo se le considera como la base del desarrollo y prueba de hipótesis de una investigación especifica

La investigación tiene un diseño no experimental y transversal, porque no se manipulan deliberadamente las variables, si no que parte de una situación existente que no es provocada intencionalmente.

3.1.4 Enfoque

El enfoque utilizado fue Cuantitativo, ya que se usa la recolección de datos de los fenómenos ocurridos.

3.2 Población y Muestra

3.2.1 Población

La población estará conformada por todos los trabajadores de la empresa de telecomunicaciones, las cuales fueron 10 entre técnicos y auxiliares. El esquema del diseño de la investigación tuvo la siguiente estructura:

M → O

Donde:

M = Muestra

O = Observación

3.2.2 Muestra

Por su parte Hernández citado en Castro (2003), expresa que "si la población es menor a cincuenta (50) individuos, la población es igual a la muestra" (p.69). Motivo por el cual la muestra seria de 10 personas.

3.3 Técnicas de recolección de datos

A. Técnica

Se recogerá la información a través de una encuesta.

Las encuestas nos permitirán explorar cuestiones dadas para la obtención de resultados. Estas encuestas estuvieron dirigidas a las personas que trabajan en la empresa de telecomunicaciones.

B. Instrumentos

En la presente investigación se aplicará una encuesta de 10 preguntas a los técnicos y asistentes de la empresa.

3.4 Técnicas para el procesamiento de la información

Durante la recolección de datos se realizan las siguientes actividades: Se aplican encuestas a una muestra de la población de la empresa. Tras la recogida de información mediante herramientas de investigación, se han descrito las características de la solución propuesta. Se realiza un análisis integral sobre la base de juicios críticos desvinculados del marco teórico, objetivos y variables de investigación, y conceptos técnicos extraídos de los datos obtenidos durante el estudio.

Se realizarán encuestas en los próximos meses. Los instrumentos que

se van a aplicar son:

* Encuestas

* Observación

* Entrevistas

Para realizar las actividades mencionadas se efectuó lo siguiente:

* Se aplicaron encuestas a 10 trabajadores y al encargado de la empresa

* Las encuestas se realizarán en la empresa al personal administrativo, auxiliar y técnico.

A. Estadística inferencial

Se quiere estimar la asociación (si existe o no) entre 2 o más variables.

Proporcionará la teoría necesaria para inferir o estimar la toma de decisiones sobre la base de la información parcial mediante técnicas descriptivas. Se someterá a prueba:

- La hipótesis central
- Las hipótesis especificas

3.5 Matriz de consistencia

Se muestra en el siguiente cuadro.

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	INSTRUMENTO
Problema General ¿De qué manera Influye la Implementación de un Sistema de seguridad de la Información basado en la norma ISO 27001 en una empresa de telecomunicaciones**,** 2021? **Problemas específicos** * ¿De qué manera Influye la Implementación de un Sistema de seguridad de la Información basada en la norma ISO 27001 en la Cantidad de Incidentes de Seguridad en una empresa de telecomunicaciones, 2021? * ¿De qué manera Influye la Implementación de un Sistema de seguridad de la Información basada en la norma ISO 27001 en el Cumplimiento de nuevas normas establecidas para una empresa de telecomunicaciones, 2021? * ¿De qué manera Influye la Implementación de un Sistema de seguridad de Información basada en la norma ISO 27001 en el grado de satisfacción de los clientes con respecto al servicio que otorga una empresa de telecomunicaciones, 2021?	**Objetivo general** Determinar la influencia de la implementación de un Sistema de seguridad de la Información en la norma ISO 27001 en una empresa de telecomunicaciones, 2021. **Objetivos específicos** * Determinar la influencia de la Implementación de un Sistema de seguridad de la Información basada en la norma ISO 27001 en la Cantidad de Incidentes de seguridad en una empresa de telecomunicaciones, 2021. * Determinar la influencia de la Implementación de un Sistema de seguridad de la Información basada en la norma ISO 27001 en el Cumplimiento de nuevas normas establecidas para una empresa de telecomunicaciones, 2021. * Determinar la influencia de la Implementación de un Sistema de seguridad de la Información basada en la norma ISO 27001 en el grado de satisfacción de los clientes con respecto al servicio que otorga una empresa de telecomunicaciones, 2021.	**Hipótesis General** La Implementación de un Sistema de gestión de seguridad de la Información basado en la norma ISO 27001 Influye en una empresa de telecomunicaciones, 2021. **Hipótesis específicas** * La Implementación de un Sistema de gestión de seguridad de la Información basado en la norma ISO 27001 Influye en la Cantidad de Incidentes de Seguridad en una empresa de telecomunicaciones, 2021 * La Implementación de un Sistema de gestión de seguridad de la Información basado en la norma ISO 27001 Influye en el Cumplimiento de nuevas normas establecidas para una empresa de telecomunicaciones, 2021 * La Implementación de un Sistema de gestión de seguridad de la Información basado en la norma ISO 27001 Influye en el grado de satisfacción de los clientes con respecto al servicio que otorga una empresa de telecomunicaciones, 2021	**V.I.** **Sistema de** Gestión de Seguridad d**e la Información** **V.D.: Norma ISO 27001**	* *Disponibilidad de la información* * Integridad de la información * Confidencialidad de la información * Incidentes de Seguridad * Cumplimiento de nuevas normas establecidas * Satisfacción de los clientes con respecto al servicio	*% de Reportes entregados en el plazo* % de Reportes Íntegros generados % de Reportes Confidenciales Entregados Correctamente * Cantidad de Accidentes y Enfermedades * Mejorar condiciones de trabajo * Satisfacción por el servicio	Encuesta Encuesta Encuesta Encuesta Encuesta Encuesta

CAPITULO IV: RESULTADOS

4.1 Validación y confiabilidad

4.1.1 Validación

Los cuestionarios que midieron las variables, fueron sometidas a un grupo de jueces expertos, integrados por profesionales investigadores que laboran en diferentes Instituciones Públicas y Privadas de la ciudad de Lima, este proceso es conocido también como medición de validez de contenido.

Este grupo de expertos informaron acerca de la aplicabilidad de los cuestionarios de la presente investigación y se aplicó la técnica de opinión de expertos.

Tabla 1. Escala de valoración juicio de expertos

(%)	CALIFICACION
1-29	Malo
30-59	Regular
60-89	Bueno
90-100	Muy bueno

La calificación obtenida es de 87%, se encuentra dentro del rango Bueno, es aceptado, se muestra en el anexo No 02.

4.1.2 Confiabilidad

La confiabilidad del instrumento se estima a través del coeficiente Alfa de Cronbach.

Tabla 2. Escala de valores para la confiabilidad

VALORES	**INTERPRETACION**
1,00	Confiabilidad perfecta
0,72 a 0,99	Excelente confiabilidad
0,66 a 0,71	Muy confiable
0,60 a 0,65	Confiable
0,54 a 0,59	Confiabilidad baja
Menos a 0,53	Confiabilidad nula

Tabla No 3

Resumen del procesamiento de los casos

		N	**%**
Casos	Válidos	10	100,0
	Excluidos	0	0,0
Total		**10**	

Tabla No 4

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
0,712	10

Se ha obtenido 0.712 que se encuentra en el rango de excelente confiabilidad.

4.2 Análisis estadísticos e interpretación de datos

Se analizarán la estadística de los cuestionarios de preguntas y se interpretarán con sus respectivos comentarios.

ITEM 1: ¿Ustedes están de acuerdo sobre Normativas de Seguridad de la Información?

Tabla 2. Sobre Normativas de Seguridad de la Información

		Frecuencia	%	% válido	% acumulado
Válido					
	Desacuerdo	2	20	20	20
	No sabe/no opina	1	10	10	30
	De acuerdo	7	70	70	100,0
	Total	10	100,0	100,0	

Interpretación

En la Tabla 11, que corresponde al ítem 1, se puede observar que del 100% (10) de trabajadores encuestados, el 70% refieren que están De acuerdo, y el 20 % están en desacuerdo. Por lo tanto, se desprende que el 10% no sabe/no opina.

ITEM 2: ¿Con qué frecuencia los capacitan en la identificación de incidentes de seguridad de la información durante la jornada de trabajo?

Tabla 3. Identificación de incidentes de seguridad en la jornada de trabajo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido					
	Desacuerdo	2	20	20	20
	No sabe/no op	2	20	20	40
	De acuerdo	6	60	60	100,0
	Total	10	100,0	100,0	

Interpretación

En la Tabla 12, que corresponde al ítem 2, se puede observar que del 100% (10) de trabajadores encuestados, el 60% refieren como algo De acuerdo, y el 20 % no están de acuerdo. Por lo tanto, se desprende que el 20% no sabe/no opina

ITEM 3: ¿Ustedes están de acuerdo con la política de Seguridad de la información?

Tabla 4. Política de Seguridad de la Información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido					
	Desacuerdo	1	10	10	10
	No sabe/no op	1	10	10	20
	De acuerdo	8	80	80	100,0
	Total	10	100,0	100,0	

Interpretación

En la Tabla 13, que corresponde al ítem 3, se puede observar que del 100% (10) de trabajadores encuestados, el 80% refieren como algo De acuerdo, y el 10 % no están de acuerdo. Por lo tanto, se desprende que el 10% no sabe/no opina

ITEM 4: ¿Ha sufrido algún incidente de seguridad en la jornada laboral y piden ser atendidos?

Tabla 5. actividades laborales y piden ser atendido

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido					
	Desacuerdo	2	20	20	20
	No sabe/no op	1	10	10	30
	De acuerdo	7	70	70	100,0
	Total	10	100,0	100,0	

Interpretación

En la Tabla 14, que corresponde al ítem 4, se puede observar que del 100% (10) de trabajadores encuestados, el 70% refieren como algo De acuerdo, y el 20% están en desacuerdo. Por lo tanto, se desprende que el 10% no sabe/no opina.

ITEM 5: ¿Existe alguna persona encargada de la Seguridad de la información y están de acuerdo con sus políticas?

Tabla 6. Encargada de la Seguridad Industrial y están de acuerdo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido					
	Desacuerdo	2	20	20	20
	No sabe/no op	2	20	20	40
	De acuerdo	6	60	60	100,0
	Total	10	100,0	100,0	

Interpretación

En la Tabla 15, que corresponde al ítem 5, se puede observar que del 100% (10) de trabajadores encuestados, el 60% refieren como algo De acuerdo, y el 20% no están de acuerdo. Por lo tanto, se desprende que el 20% no sabe/no opina.

ITEM 6: ¿Realizan simulacros para casos de seguridad y están de acuerdo?

Tabla 7. Simulacros para casos de seguridad y están de acuerdo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido					
	Desacuerdo	1	10	10	10
	No sabe/no op	1	10	10	20
	De acuerdo	8	80	80	100,0
	Total	10	100,0	100,0	

Interpretación

En la Tabla 16, que corresponde al ítem 6, se puede observar que del 100% (10) de trabajadores encuestados, el 80% refieren como algo De acuerdo, y el 10 % no están de acuerdo. Por lo tanto, se desprende que el 10% no sabe/no opina.

ITEM 7: ¿Se presentan incidentes de seguridad en la empresa y están de acuerdo su atención?

Tabla 8. Accidentes comunes en la empresa

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido					
	Desacuerdo	1	10	10	10
	No sabe/no op	2	20	20	30
	De acuerdo	7	70	70	100,0
	Total	1	100,0	100,0	

Interpretación

En la Tabla 17, que corresponde al ítem 7, se puede observar que del 100% (10) de trabajadores encuestados, el 70% refieren como algo De acuerdo, y el 10 % está en desacuerdo y el 20% no sabe/no opina

ITEM 8: ¿Conoce usted algún caso de seguridad y está de acuerdo con su tratamiento?

Tabla 9. Enfermedad ocupacional

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido					
	Desacuerdo				
	No sabe/no op	1	10	10	10
	De acuerdo	9	90	90	100,0
	Total	10	100,0	100,0	

Interpretación

En la Tabla 18, que corresponde al ítem 8, se puede observar que del 100% (10) de trabajadores encuestados, el 90% refieren como algo De acuerdo, y el 10% no sabe/no opina.

Prueba de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Capacidad de Respuesta	,381	10	,000	,640	10	**,000**
Fiabilidad	,381	10	,000	,640	10	**,000**
Valor percibido	,329	10	,003	,655	10	**,000**
Seguridad	,482	10	,000	,509	10	**,000**
Empatía	,329	10	,003	,655	10	**,000**
Conformidad del cliente	,381	10	,000	,640	10	**,000**
Expectativas del cliente	,329	10	,003	,655	10	**,000**

Según la prueba de normalidad para establecer si los datos recogidos se encuentran dentro de una distribución normal, en ambas pruebas (Kolmogorov-Smirnov y Shapiro-Wilk) se recogen que los datos no están dentro de una distribución normal ya que el nivel de significación se encuentra por debajo de 0,05, por lo tanto se tendrá que utilizar para la contrastación de hipótesis la estadística no paramétrica. Considerando la muestra y el tipo de variables, utilizaremos el estadístico de Rho de Spearman

Se utilizará el estadístico Rho de Spearman porque lo que se busca es la influencia de la implementación de este sistema en la empresa. Este coeficiente, al medir el nivel de asociación, nos determinar qué tan influyente será una variable sobre otra

4.3 Contrastación de hipótesis

HIPÓTESIS GENERAL

Ha: La Implementación de un Sistema de seguridad de la Información basado en la norma ISO 27001 Si Influye en una empresa de telecomunicaciones**,** 2021

H_0: La Implementación de un Sistema de seguridad de la Información basado en la norma ISO 27001 No Influye en una empresa de telecomunicaciones**,** 2021

Tabla 12**: Correlaciones**

			Sistema de Seguridad de la Información	Normas ISO 27001
Rho de Spearman	Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001	Coeficiente de correlación	1,000	0,699**
		Sig. (bilateral)	.	0,000
		N	6	6
	Empresa de telecomunicaciones	Coeficiente de correlación	0,699**	1,000
		Sig. (bilateral)	0,000	.
		N	6	6

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

A. **DECISIÓN ESTADISTICA:**

De acuerdo al resultado del procesamiento obtenido con el SPSS 23, se puede observar una alta correlación entre ambas variables que arroja el coeficiente de Spearman igual a 0.699. Para la contrastación de la hipótesis se realiza el análisis de p valor o sig. Asintótica (Bilateral) = 0.000 que es menor que 0.05, por lo que se niega la hipótesis nula y por consiguiente se acepta la Ha.

B. RESULTADO:

Se concluye en el rechazo de la hipótesis nula y la aceptación de la hipótesis general.

PRUEBA DE LAS HIPÓTESIS ESPECÍFICAS

Hipótesis específica 01:

Ha: ρ≠ 0: La Implementación de un Sistema de gestión de seguridad de la Información basado en la norma ISO 27001 Si Influye en la Cantidad de Incidentes de seguridad en una empresa de telecomunicaciones**,** 2021.

H_0: ρ =0: La Implementación de un Sistema de gestión de seguridad de la Información basada en la norma ISO 27001 No Influye en la Cantidad de Incidentes de seguridad en una empresa de telecomunicaciones**,** 2021.

Tabla 12**: Correlaciones**

			Sistema de Seguridad de la Información	Cantidad de Accidentes
Rho de Spearman	Sistema de Seguridad de la Información	Coeficiente de correlación	1,000	0,699**
		Sig. (bilateral)	.	0,000
		N	6	6
	Cantidad de Incidentes	Coeficiente de correlación	0,699**	1,000
		Sig. (bilateral)	0,000	.
		N	6	6

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

A. DECISIÓN ESTADISTICA:

De acuerdo al resultado del procesamiento obtenido con el SPSS 23, se puede observar una alta correlación entre ambas variables que arroja el coeficiente de Spearman igual a 0.675. Para la contrastación de la hipótesis se realiza el análisis de p valor o sig. Asintótica (Bilateral) = 0.000 que es menor que 0.05, por lo que se niega la hipótesis nula y por consiguiente se acepta la Ha.

B. RESULTADO:

Se concluye en el rechazo de la hipótesis nula y la aceptación de la hipótesis

Especifica 1.

Hipótesis específica 02:

Ha: ρ≠ 0: La Implementación de un Sistema de gestión de seguridad de la Información basada en la norma ISO27001 Si Influye en el cumplimiento de nuevas normas establecidas para una empresa de telecomunicaciones**,** 2021.

H_0: ρ =0: La Implementación de un Sistema de gestión de seguridad de la Información basada en la norma ISO27001 No Influye en el cumplimiento de nuevas normas establecidas para una empresa de telecomunicaciones**,** 2021.

Tabla 12**: Correlaciones**

			Sistema de Seguridad de la Información	Cumplimiento de Nuevas Normas
Rho de Spearman	Sistema de Seguridad de la Información	Coeficiente de correlación	1,000	0,699**
		Sig. (bilateral)	.	0,000
		N	6	6
	Cumplimiento de Nuevas Normas	Coeficiente de correlación	0,699**	1,000
		Sig. (bilateral)	0,000	.
		N	6	6

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

A. DECISION ESTADISTICA:

De acuerdo al resultado del procesamiento obtenido, se puede observar una

alta correlación entre ambas variables que arroja el coeficiente de Spearman igual a 0.668. Para la contrastación de la hipótesis se realiza el análisis de p valor o sig. Asintótica (Bilateral) = 0.000 que es menor que 0.05, por lo que se niega la hipótesis nula y por consiguiente se acepta la Ha.

B. RESULTADO:

Se concluye en el rechazo de la hipótesis nula y la aceptación de la hipótesis especifica 02.

V. DISCUSIÓN, CONCLUSIONES Y RECOMENDACIONES

5.1 Discusión de resultados

En este capítulo, los resultados de este estudio cumplen con el propósito del estudio, teniendo en cuenta que la implementación de un sistema de gestión de seguridad de la información incide en el proceso de gestión de riesgos en una empresa de telecomunicaciones, 2021. Al respecto, el estudio de Rivero (2017) es que, en el contexto de la gestión de riesgos, los métodos de evaluación de riesgos, un tema de interés para nosotros en la investigación, también apuntan a la importancia del análisis de riesgos, utilizado de manera óptima en este estudio. . En el caso de Rodríguez (2016) en su tesis titulada "Desarrollar y desarrollar un sistema de gestión de riesgos basado en pautas establecidas por NTC-ISO 31000 2011 para Simma Ltda". Por lo tanto, el estudio realizado por Rodríguez está en el contexto de la gestión de riesgos, la capacitación para los empleados relacionados con los riesgos, un tema que representa nuestros beneficios en la investigación, requiere la importancia del análisis de riesgos, el uso óptimo de estos estudios. En este sentido, Ayala (2017) en su tesis se titula "Sistema de gestión de seguridad de la información para mejorar el proceso de gestión de riesgos en el Hospital Nacional, 2017" está en el contexto de la gestión de riesgos. El tema muestra nuestro interés en la investigación, además El análisis de riesgos es importante, el análisis de riesgos, el análisis de riesgos y el uso óptimo de estos estudios. Las metas alcanzadas establecen que lo que señala Kano (2011), la disciplina nos dice sobre riesgos, peligros, análisis de escenarios, mejores prácticas y marcos regulatorios nos obligan a brindar niveles de procesos y tecnología para incrementar la confianza en la creación, uso, almacenamiento, transmisión, recuperación y eventual eliminación de información. Según ISO 31000 (2009), esto significa que las actividades de una organización implican riesgos. Las organizaciones deben gestionar el riesgo identificando, analizando y evaluando si es necesario modificar el riesgo tratando el riesgo para

cumplir con sus criterios de riesgo, donde se ha logrado el objetivo general, de una manera que pueda reducir el riesgo mediante la implementación de la seguridad de la información. sistema. Para evaluación de riesgos, ISO 31000 (2009).

VI. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

En primer lugar, la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 afecta a las empresas de telecomunicaciones, en el año 2021. En segundo lugar, la implementación de un sistema de gestión de seguridad de la información basado en las normas ISO 2700 afecta el número de incidentes de seguridad en la empresa de telecomunicaciones, año 2021, con base en datos estadísticos para el valor de prueba menos que el error. En tercer lugar, la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 2700 afecta el cumplimiento de los nuevos estándares fijados para las empresas de telecomunicaciones 2021. Así lo confirma el procedimiento de Spearman, donde se evaluó la comparación de los dos grupos mediante la prueba de Spearman. significativo. En cuarto lugar, la implementación de un sistema de gestión de seguridad de la información conforme a la norma ISO 27001 incide en el nivel de satisfacción de los clientes con los servicios prestados por las empresas de telecomunicaciones, en el año 2021.

6.2 Recomendaciones

Primero, en las empresas de telecomunicaciones, la gestión de TI debe estar alineada con las estrategias comerciales (es decir, lo que el negocio quiere). Se debe mantener la gestión de la seguridad de la información, asegurando la confidencialidad, integridad y disponibilidad así como la calidad para soportar las decisiones de negocio, exigiendo a la organización alinear todos sus recursos y cada recurso de gestión de riesgos (amenazas y vulnerabilidades). para que se puedan aplicar los controles apropiados y los riesgos se mantengan en un nivel aceptable. En segundo lugar, se debe implementar un sistema de gestión de la seguridad de la información para que la eficacia de los controles establecidos se pueda monitorear de manera adecuada y se puedan usar diferentes metodologías estándar para proteger los productos de información. En

tercer lugar, se recomienda que el responsable de seguridad de la información (especialista en seguridad) elabore un plan de acción o mejore las medidas de control necesarias para manejar el riesgo por severidad, se recomienda a las empresas de telecomunicaciones gestión de riesgos, evaluación de riesgos, impacto. Deben seguir un proceso de tratamiento de riesgos para que la gerencia pueda determinar las opciones de tratamiento a realizar (transferir, evitar, reducir o aceptar el riesgo).

CAPITULO VII: REFERENCIAS

7.1 Fuentes bibliográficas

* Laudon, K & Laudon, J. (2004) *Sistemas de Información Gerencial*. Octava Edición. México. Editorial Pearson –Prentice Hall

* Whiten, J. L., (2008) *Análisis de sistema: diseño y métodos*, México, McGraw-Hill/ Interamericana Editores.

* Kendall, Keneth E. (2005), *Análisis y diseño de sistemas*, México, Editorial Prentice Hall.

* Domínguez Coutiño, L.A. (2012) Análisis *de sistemas de información.* Primera Edición. México. Editorial Tercer Milenio SAC

* Andreu, R., Ricart, J. y Valor, J. (1996). *Estrategia y Sistemas de Información*. España. McGraw-Hill. Instituto de Estudios Superiores de la Empresa.

* Senn, J. (1992). *Análisis y Diseño de Sistemas de Información*. Segunda Edición. México. McGraw - Hill Interamericana.

Celí. E. (2016). *La gestión de riesgo TI y la efectividad de los sistemas de seguridad de información: caso de procesos críticos en las pequeñas entidades financieras de Lambayeque. Pueblo Cont. 27(1). 73-84.* Recuperado de:http://journal.upao.edu.pe/PuebloContinente/article/download/395/360

Areitio, J. (2008). *Seguridad de la información Redes, informática y sistemas de información. (C. L. Carmona, Ed.) Madrid España*: Ediciones Paraninfo.

Ayala , M. (2017). *Sistema de gestión de seguridad de información Para mejorar el proceso de gestión del riesgo En un hospital nacional, 2017.* Tesis, Universidad César Vallejo, Lima Perú.

Bernaldo, N. (2016). *Sistema de gestión de seguridad de la Información en el Proceso de Registros Civiles de RENIEC. San Borja. Lima 2016*. Tesis, Universidad César Vallejo, Lima.

De La cruz, R. (2016). *Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la municipalidad provincial de Paita; 2016*. Tesis, Universidad Católica Los Ángeles Chimbote, Piura.

Díaz, R. (2015). *Apoyo al proceso de implementación de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001:2013 en la alcaldía de Pasto.* Tesis, Universidad de Nariño , Colombia.

Mera. A. (2014). *Diseño del modelo de gestión de seguridad de la información del sistema ERP de EP PETROECUADOR de acuerdo a norma ISO/IEC 27002 y COBIT 5*. (Tesis de Maestría). Universidad. Ecuador. Recuperado de:http://repositorio.espe.edu.ec/bitstream/21000/8073/1/T-ESPE047641.pdf

Rios , J. (2014). *Diseño de un Sistema de Gestión De Seguridad de Información para una Central Privada de Información de riesgos*. Tesis, Pontificia Universidad Católica del Perú, Lima Perú.

Ramírez. G. y Álvarez. E. (2003). *Auditoría a la gestión de las Tecnologías y sistemas de Información. Industrial Data. 6(1). 99-102*. Recuperado de: http://sisbib.unmsm.edu.pe/bibvirtualdata/publicaciones/indata/Vol6_n1/pf/ auditoria.pdf

* Talavera Álvarez, V.R. (2013). Tesis: *Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013.*

Tesis para optar por el Título de Ingeniero Informático, Pontificia Universidad Católica del Perú, Lima, Perú.

* Gonzáles López, C. M. (2016). Tesis: *Desarrollo e Implementación de un Sistema de Información para el control del proceso de capacitación de una empresa del rubro de las telecomunicaciones en el Perú*. Tesis para optar por el Título de Ingeniero Informático, Universidad Católica Sedes Sapientiae, Lima, Perú.

7.2 Fuentes Electrónicas

Cáceres, E.A. (2014) *Análisis y Diseño de Sistemas de Información*. Recuperado de http://www.facso.unsj.edu.ar/catedras/ciencias-economicas/sistemas-de-informacion-II

ANEXOS

Anexo N° 1

CUESTIONARIO

I. PRESENTACIÓN

Estimado (a) señor (a), el presente cuestionario es parte de una investigación la cual tiene por finalidad obtener información, acerca de la recolección de datos para las Variables del estudio.

II. INSTRUCCIONES

- Este cuestionario es anónimo. Por favor responda con sinceridad.
- Escriba a que área pertenece, lea detenidamente cada ítem. Responda el ítem y ponga una escala valorativa que se muestra en el cuadro.
- Gracias por su colaboración.

Área: _____

Si cumple	No cumple	Parcialmente cumple	No aplica
4	3	2	1

		4	**3**	**2**	**1**
1.	Capacidad de respuesta				
2.	Fiabilidad				
3.	Seguridad				
4.	Empatía				
5.	Valor percibido				
6.	Expectativas del cliente				
7.	Conformidad del cliente				

Anexo 2

Formato para la Prueba de Validez del Instrumento

VALIDEZ DEL INSTRUMENTO

Viene a ser el grado en que el instrumento puede medir a la variable a la que se pretende medir.El instrumento a utilizarse para recolectar información es una Encuesta con diversas preguntas, un cuestionario elaborado con los indicadores de la variable en estudio, el mismo que se somete a una consulta de Opinión a Investigadores Expertos en el área, quienes nos proporcionan sus respectivas opiniones.

MATRIZ DE ANALISIS DE JUICIO DE EXPERTOS

CRITERIOS	**JUECES**			**Total**
	1	**2**	**3**	
Claridad:	**4**	**4**	**4**	**12**
Objetividad:	**4**	**4**	**5**	**13**
Actualidad:	**3**	**4**	**4**	**11**
Organización:	**4**	**4**	**5**	**13**
Suficiencia:	**5**	**5**	**4**	**14**
Intencionalidad:	**5**	**5**	**4**	**14**
Consistencia:	**4**	**4**	**3**	**11**
Coherencia:	**4**	**5**	**5**	**14**
Metodología:	**5**	**4**	**5**	**14**
Pertinencia:	**4**	**5**	**5**	**14**
Total	**43**	**45**	**42**	**130**

CALIFICACION

INTERVALO	**INTERPRETACION**
[0.01-0.20>	Muy Baja
[0.21-0.40>	Baja
[0.41-0.60>	Moderada
[0.61-0.80>	Alta
[0.81-0.94]	Muy Alta

Total máximo = (N° criterios) x (N° de Jueces) x (Puntaje Máximo de Respuesta).

CALCULO DEL COEFICIENTE DE VALIDEZ

Validez = 130/10*3*5 = 130/150

Validez = 0.87

CONCLUSION: El coeficiente de Validez del Instrumento nos da 87%, considerado como **Bueno**