Universidad Norbert Wiener

FACULTAD DE INGENIERÍA Y NEGOCIOS
ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍAS

Tesis

Análisis de la seguridad informática de una mediana empresa Lima 2019-2020

Para optar el grado académico de Bachiller en Ingeniería de Sistemas e Informática

AUTOR

Guevara Lunarejo, Martin Cristian

ORCID: 0000-0001-9051-7131

LÍNEA DE INVESTIGACIÓN GENERAL DE LA UNIVERSIDAD

Ingenierías de Sistemas e Informática, Industrial y Gestión Empresarial y Ambiental

LÍNEA DE INVESTIGACIÓN ESPECÍFICA DE LA UNIVERSIDAD

Seguridad en Base de Datos

LIMA - PERÚ

2020

Miembros del Jurado

Presidente del Jurado

Dr. Jose Luis Herrera Salazar

Secretario

Dr. David Flores Zafra

Vocal

Mtro. Cesar Antonio Porras Ramirez

Asesora temática

Dra. Irma Milagros Carhuancho Mendoza

ORCID: 0000-0002-4060-5667

Asesor temático

Dr. Fernando Alexis Nolazco Labajos

ORCID: 0000-0001-8910-222X

Dedicatoria

En primer lugar, a Dios quien me brindó sabiduría, salud y determinación en todo momento, a mi familia que siempre me dio su apoyo especialmente a mi madre Lidu y mi tía Soledad que vieron en mí a un profesional capaz de seguir con esta carrera.

Agradecimiento

Agradezco a Dios por toda la perseverancia y bendiciones recibidas, asimismo todos de los que recibí su apoyo sostenido para que esto sea posible, profesores, mi familia y amistades. A mi asesora de tesis Dra. Irma Milagros Carhuancho Mendoza por su paciencia, enseñanza y dedicación en el proceso de la elaboración del trabajo de investigación, a la Universidad Norbert Wiener por la formación durante esta etapa universitaria.

Declaración de Autoría

Universidad Norbert Wiener	DECLARACIÓN DE AUTORIA		
	CÓDIGO: UPNW-EES-FOR-017	VERSIÓN: 01 REVISIÓN: 01	FECHA: 13/03/2020

Yo, Guevara Lunarejo Martin Cristian estudiante de la escuela académica profesional de Ingenierías de la Universidad Privada Norbert Wiener, declaro que el trabajo académico titulado: "Análisis de la seguridad informática de una mediana empresa Lima 2019-2020" para la obtención del Grado académico de Bachiller en de Ingeniería de Sistemas e Informática es de mi autoría y declaro lo siguiente:

1. He mencionado todas las fuentes utilizadas, identificando correctamente las citas textuales o paráfrasis provenientes de otras fuentes.
2. No he utilizado ninguna otra fuente distinta de aquella señalada en el trabajo.
3. Autorizo a que mi trabajo puede ser revisado en búsqueda de plagios.
4. De encontrarse uso de material intelectual ajeno sin el debido reconocimiento de su fuente y/o autor, me someto a las sanciones que determina los procedimientos establecidos por la UPNW.

.....
Firma
Guevara Lunarejo Martin Cristian
DNI: 45679790

Lima, 24 de agosto de 2020.

Huella

Índice

Índice de tablas

Índice de figuras

Pág.

Resumen

La siguiente investigación titulado Análisis de la seguridad informática de una mediana empresa, Lima 2019-2020 se elaboró con el propósito de analizar la situación actual, que puede encontrarse en una empresa todo respecto a la falta de privacidad de la información.

En la investigación se empleó el método de triangulación, también se empleó el enfoque cualitativo, analítico e inductivo que consiste en la recopilación de datos de las unidades informantes que en este caso fueron cinco actores, mediante la entrevista, lo cual nos permitirá a identificar la situación actual, obteniendo resultados para salida a las problemáticas identificadas y recomendaciones sobre la seguridad informática de la empresa, los datos fueron procesados en el programa Atlas.ti 8.

Se logró conseguir que, en una mediana empresa, no hay control definido de seguridad informáticas por falta de compromiso de otras áreas y alta gerencia, no cuentan con área de TI, no están definidos los procesos de seguridad de información, no hay políticas establecidas y no se dispone de manual para ejecutar dicha tarea. No cuenta con una privacidad informática especializada, los únicos controles que hay operativos son las actualizaciones de los antivirus y del Update. La empresa no cuenta con la madurez para la gestión de seguridad informática.

Palabras clave: Análisis, seguridad informática, triangulación, control, procesos y área de TI.

Abstract

The following research entitled Analysis of the computer security of a medium-sized company; Lima 2019-2020 was prepared for the purpose of analyzing the current situation, which can be found in a company all regarding the lack of privacy of the information.

The research used the triangulation method, the qualitative, analytical and inductive approach was also used, which consists in the collection of data from the reporting units, which in this case were five actors, through the interview and documentary review to obtain information, which will allow us to identify the current situation, obtaining results for exit to the problems identified and recommendations on the computer security of the company, data were processed in the Atlas.ti 8 program.

It was achieved that, in a medium-sized company, there is no defined control of computer security due to lack of commitment from other areas and high management, no IT area, no information security processes are defined, there are no policies in place and there is no manual to perform this task. It does not have a specialized computer privacy, the only controls that there are operating are the updates of the antivirus and the Update. The company does not have the maturity for IT security management.

Keywords: Analysis, computer security, triangulation, control, processes and IT area.

I. INTRODUCCIÓN

Al referirnos a la seguridad informática indicamos que es más que un problema de seguridad de datos que se pueden presentar en diversos dispositivos, es por ello que la S.I. está orientada al resguardo de la propiedad intelectual, así como de la información importante de las organizaciones y personas. Al hablar de S.I. es inevitable no hacer referencias a los riesgos de información el cual consta de amenazas y vulnerabilidades que se encuentran presentes en las organizaciones, estás están íntimamente involucradas y sin ambas no existiría los riesgos, también se debe tomar en cuenta que esta puede provenir del cuerpo interna o externa de las organizaciones (Tarazona, 2007).

Las Organizaciones requieren una estabilidad y un alto grado de protección el cual esté enfocada a la seguridad informática buscando prevenir las diversas amenazas dirigidas a su información. Así como existen diversas amenazas también existen diversas maneras para proteger la información; sin embargo, la principal amenaza es la desinformación que hay en las organizaciones para una correcta toma de decisiones, siendo este el motivo por el cual es necesario que las organizaciones desarrollen un modelo que permita establecer una buena práctica de la seguridad en los equipos, llevando esto a tener una correcta información, estrategias y planes para poseer una alta seguridad de información (Muñoz & Rivas, 2015).

La presencia del DevOps es cada vez más importante en las empresas u organizaciones, puesto que una de sus principales funciones es reforzar la relación entre los profesionales del TI y los desarrolladores de software cuyo fin es acortar el proceso del proyecto, a su vez permite generar estrategias para el flujo de trabajo, control de versiones y entrega de producto de software, esta técnica tiene como una de sus finalidades desarrollar diversos sistemas de información en múltiples tecnologías como por ejemplo para internet, celulares y servicios de almacenamiento en la nube, entre otras (Díaz & Muñoz, 2018).

En la empresa industrial no se maneja una sola data ni tampoco hay una buena metodología de análisis de datos ya que guardan una información repetitiva y al realizar un Backup toma más tiempo por el bajo rendimiento de las maquinas, al tener mucha información el sistema se satura.

Así mismo, actualmente hay un nivel de seguridad informática baja en la empresa, ya que se trabaja con computadoras sin licencia de antivirus, al abrir correos sospechosos se corre el riesgo la información, por la baja protección no se hace copias de seguridad o se realiza mal, no se cuenta con la criptografía asimétrica ni cuentan con la norma ISO 27000 ya que es caro al implementar ni tampoco hay el personal capacitado para su implementación. Finalmente, los errores más comunes que ocurren al momento de cargar los datos como la migración de datos están vinculados a un daño en el hardware o en el tráfico de red ocasionando así campos faltantes como información incompleta en diversos archivos y que se crea una ineficiencia en la entrada de datos lo cual nos indicaría que no cuenta con un sistema ERP.

Para la investigación se revisó trabajos previos a nivel internacional, Reyes Mena, Fuertes Díaz, Guzmán Jaramillo. (2017), se diseñó una solución implementada a través de Business Intelligence que actúa como un factor estratégico en el análisis de vulnerabilidad de un CSIRT y esto fue posible aplicando la metodología de Investigación-Acción y las fases de Ralph Kimball, igualmente Stanley Ndungu, Kenneth Wanjau, Robert Gichira, Waweru Mwangi. (2017). Evidenciaron que el estudio sobre la Teoría integrada del sistema de gestión de la seguridad de la información, identificaron la evaluación de riesgos de seguridad de la información como uno de los factores de éxito de la gestión de la seguridad de la información. Por otra parte, Allassani (2014), constata que la mayoria del personal no tiene buenos hábitos de lectura sobre las políticas de seguridad de la empresa, Los empleados que han trabajado menos de 5 años tienen menos probabilidades de leer, incluso si son personas mayores, los ejecutivos están involucrados en el proceso de monitoreo, en base que los empleados al no tener buenos hábitos de lectura, se desea recomendar que a los empleados sean evaluados anualmente y ser recompensados. Igualmente, Roratto, Dotto Dias (2014), evidenciaron que se presenta la importancia de garantizar la seguridad, inviolabilidad e integridad de la información contenida en un sistema de gestión informatizado, se concluye que, con la creciente dependencia de los sistemas críticos de almacenamiento de datos, desarrollar nuevas soluciones para el monitoreo y protección de estos datos y desarrollar nuevas soluciones, está claro que esta es un área de estudio muy prometedora e importante, y se recomienda Realizar nuevas investigaciones en el área de control y seguridad de la información a través del uso de las tecnologías de BI. Últimamente, Knorst, Vanti, Espín Andrade, Silvio (2011), evidenciaron que es posible establecer una relación utilizando estratégicamente los criterios de seguridad e integrarlos a través del modelo BSC, COBIT e

ISO27002 ya que estos facilitan el mapeo de objeticos genéricos para el negocio de TI desde la perspectiva del BSC con los objetivos generales de TI.

Asimismo, se revisó trabajos a nivel nacional, Lavado (2019), evidenció que la banca es uno de los sectores económicos que más importancia debe darle a la seguridad informática. Esto se debe a que el banco ya tiene implementado otros estándares como la ISO/IEC 27001 y Ley de Protección de Datos (Ley N° 29733), los cuales coinciden con algunos requerimientos de la norma PCI DSS. Por lo que este estándar no reemplaza, los ya implementados, si no, los complementa para darle más seguridad a la organización. Igualmente, Contreras & Vega (2019) demostraron que se presenta la planificación que garantiza el correcto funcionamiento de la solución Privileged Access Manager. La cual permite disminuir el riesgo interno de seguridad informática con los activos de TI y tiene la trazabilidad de todas las actividades realizadas por los administradores del área de redes, seguridad y base de datos de la empresa. También, Cruz & Fukusaki (2017) demostraron que un Sistema de Gestión de Seguridad de la Información puede ser implementada a diversas empresas sin tomar importancia al tamaño o rubro en el que se desempeñe, asimismo identificaron distintos métodos para reducir los riesgos que se presenten en las organizaciones, entre estos existen los mapeos de riesgos, declaración de aplicabilidad y la implementación de controles. De esta manera, Chauca Huaman (2017) demostró que la propuesta de un aplicativo web para la gestión de las auditorías informáticas para la empresa Calzado Atlas S.A. es viable luego del análisis económico, análisis de ahorro en gasto de incidentes del área de TI y análisis de rentabilidad, como solución informática para la necesidad que presenta. Finalmente, Fernández & Pacheco (2014), acreditan que el resultado es minimizar los riesgos, amenazas y vulnerabilidades de los activos de información como también el compromiso del personal de la comandancia con respecto a la seguridad de información.

La teoría de la información está considerada parte de la teoría de la probabilidad, con amplios potenciales para los sistemas de comunicación, esta teoría al igual que otras también cuenta con un origen físico que fue elaborado por científicos de la comunicación, estos buscaban estudiar la estructura estadística de los equipos de comunicación eléctrica, sin embargo esta fue empleada de manera anticipada en zonas marginales, es por ello que las últimas investigaciones realizadas hace 5 o 6 años demuestran que es necesario realizar investigaciones profundas sobre los fundamentos de esta disciplina. Asimismo, se requiere

reflexionar ciertos problemas interrelacionados con el sistema de comunicación. Para que se pueda realizar, en primer lugar, es esencial mostrar los diversos elementos involucrados como entidades matemáticas y se clasifica en 3 categorías “discreta, continua y mixta”. Por el método discreto significa que gracias a la secuencia de símbolos se logra crear mensajes y señales, de esta manera se obtiene la telegrafía, el cual está compuesto por un grupo de letras con el cual se crean palabras, a su vez se hace el uso de puntos, guiones y espacios llevando todo ello transmitir un mensaje claro y comprensible, siendo este conocido como el método continuo, además de este método existe el método mixto el cual está constituido por variables discretas y continuas (Shannon, Warren, 1948; Fazlollah, 1994). La teoría de la información es conocida como la matemática de la comunicación, es una rama de las teorías de la matemática y de la ciencia de la computación, aplicando así, esta última estudia la información relacionada a la medición y capacitación de los sistemas de comunicación para así transmitir y procesar dicha información, aplicando así un canal de información, comprensión de datos y criptografía. En este sentido desde la perspectiva de la teoría de la información es importante y necesaria que el personal tenga capacitación adecuada para emplear las estructuras de redes de telecomunicación.

Asimismo, otra teoría importante es la teoría general de Sistemas (TGS) es considerada como una ciencia de la totalidad porque cuyas propiedades aplicables a una simple adición de las partes o componentes, además el sistema mantiene su importancia incluso en donde no pueda ser formulada matemáticamente, es decir, esta no deja de ser un modelo en lugar de ser una construcción matemática, así mismo se puede decir que la TGS no busca analogías vagas y superficiales ya que estas tienen poco valor debido a la diferencia con otros fenómenos. El isomorfismo es el resultado de la abstracción y modelos conceptuales que coincide con diferentes fenómenos. Para hablar de un sistema es necesario cumplir los siguientes requisitos: Funcional y No Funcional, si estas características no se cumplen pondrían en duda el carácter de objeto del sistema, así mismo se menciona que también se pueda hacer referencia a un sistema a un conjunto de características. Por lo tanto, al indicar que existe un sistema hablamos que el objeto de investigación posee de ciertas características que valoran el concepto de sistema.

Así mismo la definición de sistema busca abstraer y comparar diversos hechos que sean diferentes (Bertalanffy, 1976; Luhmann, 1996). La teoría general de sistemas genera

herramientas para la aplicación en cualquier tipo de sistemas y en cualquier tipo de organización, es posible identificar los elementos de la TGS en cualquier tipo de empresa así ayudando a los administradores a entender el fundamento de su negocio. Nos permite llevar un análisis y desarrollo del sistema con el objetivo de buscar la solución que sea las mismas características del sistema y así se podrá lograr los objetivos de la organización.

De esta forma, el estudio se sustenta con la teoría de la decisión es crear todas las posibles hipótesis sobre la toma de decisiones racional, las teorías descriptivas tienen como finalidad explicar y predecir el cómo es que la gente toma las decisiones, esta es una disciplina empírica por lo tanto es basada en la experiencia y realidad, es por ello que proviene de la psicología experimental. El objetivo de las teorías normativas es producir prescripciones sobre la responsabilidad de la toma de decisiones, la teoría de decisiones descriptivas y normativas tienen diversas diferencias generando estas que se estudien independiente cada una. Por lo tanto para que en una organización existan una especialización horizontal, es necesaria la especialización vertical, ya que ambas permitirán llevar una coordinación eficaz entre los empleados, además la especialización horizontal permite a los empleados desarrollar mayores habilidades y destrezas para así realizar sus labores, por otro lado la especialización vertical da pie a generar una mejor destrezas para una correcta toma de decisiones, generando en el personal una responsabilidad sobre sus decisiones ante un consejo administrativo, un cuerpo legislativo o cualquier otro (Herbert, 1997; Peterson, 2009). Esta teoría ayudó ver que el personal representa una pieza importante al ejecutar el proceso de decisión al realizar sus labores y que los decisores tengan habilidades estratégicas para una mejor destreza en la toma de decisión. Al mismo tiempo, Con la teoría de decisiones se analizará y hará frente a cada problema que la empresa obtenga puesto que el personal tendrá la capacidad y experiencia que se requiere.

En este mismo se ha conceptualizado sobre la seguridad informática, para poder brindar una buena seguridad informática y evitar su vulnerabilidad, es necesario una buena gestión, un buen sistema de información, servicio y redes ya que todos estos nos permitirán identificar si es que existe alguna irregularidad en la seguridad informática. La Open Source Security Testing Methodology Manual (OSSTMM) es una metodología que usa como base el testeo manual que busca reducir las limitaciones que puedan presentarse entre los activos de información que se buscan proteger y las posibles porosidades de seguridad informática.

La seguridad informática es imprescindible ya que este asegura la disponibilidad, privacidad e integridad de la información, para esto existe diversas técnicas, siendo una de ellas la criptografía la cual consiste en transformar un mensaje descifrado que con la ayuda de claves podrá ser descifrado.

El sistema de información ha ido evolucionando desde sus inicios, requiriendo la formación de profesionales responsables de evaluar un correcto funcionamiento en el área de informática, así mismo buscan identificar los puntos débiles que necesiten aplicar medidas preventivas y correctiva para así reducir las probabilidades de una perdida de información, tomando en cuenta que estas pérdidas causan costos importantes en la organización. La seguridad informática hoy en día es de suma importancia para las compañías, organizaciones, establecimientos privadas y públicas; de tal manera que el uso de esta ha llegado a incluir diversas actividades profesionales y humanas al nivel mundial ya que las redes de comunicación y los sistemas de comunicación ayudan al crecimiento social y económico de las naciones (Proaño, Gavilanes, 2018; Gordón, Pacheco, 2018; Solís, Pinto, Solís, 2017; Tirado, Álvarez, Carreño, Ramos, 2017; Gil, Gil, 2017).

Para obtener la evidencia digital necesaria se empleará la guía metodológica, esta nos permitirá realizar un proceso en la cual no se comprometerá la confidencialidad e integridad y se llevará a cabo con la norma ISO/IEC 27037 (2012), esta misma menciona que la cadena de custodia ocupa un papel muy importante en la investigación, además hace referencia que se debe saber y comprender cada paso que se realiza en el mano de las pruebas digitales, en consecuencia se brinda una correcta confidencialidad y credibilidad del proceso, teniendo así una custodia limpia y sin negligencias. Aplicando la metodología OSSTMM y Ethical Hacking, se dispone en la verificación para estimar el impacto y criticidad de las vulnerabilidades halladas, además se medirán los riesgos de la seguridad informática que se encuentran en los canales de información usando la metodología ya antes mencionada y herramientas apropiadas para evaluar la seguridad operacional, por ejemplo: los factores humanos, factores físicos, redes inalámbricas, servicios, aplicaciones, y redes de datos. Con la seguridad informática se deberá mejorar los procesos para un intercambio seguro de información, para obtener este resultado se deberá combinar diversas técnicas como por ejemplo la esteganografía el cual se encarga de ocultar mensajes u objetos dentro de otras llamadas portadores para ser enviada, a su vez hace uso de la criptografía. De la misma

forma, se debe acelerar los procesos en los cifrados y descifrados, lo que implicaría una mayor seguridad en menor tiempo. De la misma manera, en el área de TI con el profesionalismo del personal evaluarán el correcto funcionamiento del sistema de información para que los ataques con botnetes no sean introducidos al sistema, así los hackers no tomen control remoto, de esta manera no se convierta la principal amenaza para la red de datos de la empresa. Las Organizaciones contaran con un plan que guíe los esfuerzos de protección de información, deberán aprender a determinar la calidad óptima de inversión en seguridad informática, así desarrollará modelos de simulación que permitan evaluar el nivel óptimo de seguridad.

Es preciso señalar, que la seguridad de la informática de una empresa cumple un papel muy importante para garantizar la privacidad e integridad de la información y se requiere de profesionales en el área informática responsables de evaluar su correcto funcionamiento. En tal sentido, las subcategorías son: a) Privacidad de la información, según (SOTO, 2017; Gregorio & Ornelas 2011; Romero 2017), la privacidad de la información en muchas ocasiones es vulnerada por diversas sociedades que van en aumento, esto se debe a que la información brindada sea utilizada como un elemento o dispositivo por la cual tienen un control total para el manejo de esta, por ejemplo: al registrar los datos personales en una red social se pierde el control absoluto de dicha información es por ello que existe la probabilidad que sea filtrada, duplicada o transferida. Así mismo tomando en consideración lo personal o publico existen ciertos márgenes en lo que se evidencia la fuga de información, esta información puede ser manejada por pequeñas cantidades de personas, sin embargo, estas serían responsables de difundirlas a un gran número de personas siendo este, un riesgo. Por último, se puede indicar que todo esto se debe a la falta de límites en el mundo digital por lo tanto es necesario que los datos personas o cualquier tipo de información privada cumpla con un riguroso control de procesamiento; b) Responsabilidad en el funcionamiento de la información (ISO/IEC 27000: 2014 - 3.2.1; ISO/IEC 27000: 2014 - 3.2.5; ISO/IEC 27000: 2014 - 3.2.3), se refiere a un sistema de gestión de seguridad de la información (SGSI) es necesario mencionar que está compuesto por políticas, procedimientos, directrices, recursos asociados y actividades con la finalidad de proteger los activos de información que la organización posee, al mencionar el SGSI hablamos de un enfoque sistemático el cual busca establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información ya que esta es necesaria para que las organizaciones

puedan alcanzar sus objetivos de negocio, así mismo se puede indicar que la base para un buen SGSI es la evaluación de los riesgos y los diversos niveles de aceptación ante estos, igualmente es necesario implementar ciertos los controles que asegure que se cumplan los objetivos específicos para poder asegurar la información que posee, a su vez es creada para tratar y gestionar de manera correcta los riesgos que surjan en la organización, además se puede indicar que el sistema de gestión conoce los recursos que guiaran o ayudaran a lograr los objeticos de la organización.

El estudio tiene justificación teórica porque se sustenta que en la teoría de información nos permite comprender la importancia del procesamiento de la información, ya que esto nos da acceso a ver la capacidad de los sistemas de comunicación y de poder transmitir o procesar la información; asimismo la teoría de sistemas permite entender que para el análisis se debe tener una mentalidad sistémica, porque al tener una mente sistémica podemos ver, analizar, actuar y entender el problema real; de igual modo la teoría de decisión permite conocer el valor significativo de la toma de decisiones para cualquier tipo de desafío, porque al tomar una decisión hay diversos factores y así tomar el mejor resultado posible siendo así un resultado positivo.

El estudio tiene justificación práctica porque permite identificar las deficiencias en base a la seguridad informática en descoordinación entre las áreas, para determinar en donde se encuentra la duplicidad de datos de información; asimismo se identifica las vulnerabilidades de un posible ataque cibernético, nos permite identificar cuáles son las malas configuraciones del sistema para utilizar un exploit especifico; del mismo modo determina un mejor control de la información, para identificar el cuello de botella del tráfico de datos.

El estudio tiene justificación metodológicamente porque se realizó bajo el enfoque cualitativo, el estudio se basa en un caso particular, como lo es en la empresa de estudio, también se basa en los datos que surgen poco a poco, asimismo permite obtener las perspectivas de las personas involucradas directamente con la investigación y el problema se analiza dividido en partes. En ese sentido, las técnicas e instrumentos usadas fueron: el análisis documental, que consta en examinar los datos ya existentes, la técnica Delphi busca obtener información esencial para la toma de decisiones, las entrevistas es una de las técnicas

que busca la apreciación de la opinión respecto al problema y los cuestionarios es una de las técnicas que busca obtener datos precisos.

Para el estudio se formuló el siguiente problema general: ¿Cuál es la situación de la seguridad informática de una mediana empresa, Lima 2019-2020?; asimismo se planearon los problemas específicos: a) ¿Cuál es la situación de la privacidad de la información de una mediana empresa, Lima 2019-2020?; b) ¿Cuál es la situación de la responsabilidad en el funcionamiento de la información de una mediana empresa, Lima 2019-2020?

Del mismo modo, el objetivo general es proponer analizar la seguridad informática de una mediana empresa, Lima 2019-2020, del mismo modo los tenemos como objetivos específicos: a) Analizar la privacidad de la información de una mediana empresa, Lima 2019-2020; b) Analizar la responsabilidad en el funcionamiento de la información de una mediana empresa, Lima 2019-2020.

II. MÉTODO

2.1 Enfoque y diseño

El estudio se sustentó en el enfoque cualitativo, el cual se define como aquel que utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación (Hernández, Fernández, & Baptista, 2014). Este método se aplicó porque se entrevistó al personal relacionado con el problema de la seguridad informática de una pequeña empresa, y se tomarán sus respuestas como válidas para la investigación.

Asimismo, el método utilizado fue el estudio de caso, determinado como aquel que investiga, analiza una situación o problemática de manera individual dentro de una sociedad o entidad; así mismo, el lugar donde interactúan diferentes personas, tiene por finalidad de entender su relación (Stake, 1999). Por dicha razón que se aplicó en la investigación porque se analizó el problema en particular; en este caso, en esta pequeña empresa y sirvió para que esta entidad comprenda las carencias que tiene y que afectan en la seguridad informática. Igualmente, se empleó el método analítico que consiste en definir la extracción de un elemento en fracciones, de las cuales tiene como objetivo estudiar, examinar de manera individual y aislada; esto es, que se pueda comprender la intercomunicación entre sí (Gomez, 2012). En este aspecto, se aplicó porque el problema de seguridad informática se observó dentro de la empresa, a través de sus sistemas y a nivel de filtración de datos relacionada con el problema.

2.2 Escenario y unidades informantes

La empresa en estudio se creó en el año 2010, se dedica a elaborar productos de panificación netamente a programas sociales en Lima y provincias, el servicio que brinda principalmente es el traslado y preparación de alimentos al programa social Qali Warma, y presenta dificultades en el área Administrativo y Logístico lo cual genera un problema con la información.

Los participantes fueron: a) Persona de género femenino, de 26 años, tiene grado de Bachiller en Ingeniería de Sistemas, es Analista de sistemas, tiene 2 años trabajando en la empresa; b) Persona de género masculino, de 28 años, tiene grado de Bachiller en Ingeniería de Sistemas, es Jefe de sistemas, tiene 7 años en la empresa; c) Persona de género masculino, de 30 años, tiene grado de Bachiller en Ingeniería de Sistemas, es Analista de

proyectos, tiene 2 años en la empresa; d) Persona de género masculino, de 26 años, tiene grado de Bachiller en Ingeniería de Sistemas, es Desarrollador, tiene 5 años trabajando en la empresa; e) Persona de género masculino, de 30 años, tiene grado de Técnico en redes y comunicaciones, tiene 3 años trabajando en la empresa.

Todos los participantes fueron seleccionados para esta entrevista, porque están involucrados con el problema que tiene la empresa, asimismo, conocen del problema.

2.3 Categorías y subcategorías apriorísticas

La seguridad de la informática de una empresa cumple un papel muy importante para garantizar la privacidad e integridad de la información y se requiere de profesionales en el área informática responsables de evaluar su correcto funcionamiento.

Tabla 1

Categorización de Seguridad de la información

Sub categoría	**Indicador**
Privacidad de la información	Habeas Data
	Análisis e identificación de los riesgos
Responsabilidad en el funcionamiento de la información	Seguridad de información
	Mantenimiento
	Outsourcing

Respecto a la tabla 1, corresponde a la categorización de seguridad de la información divide en 2 subcategorías que son: a) privacidad de la información; b) responsabilidad en el funcionamiento de la información. Cada subcategoría se disgrega en indicadores comenzando por la primera subcategoría que son: a) habeas data; b) análisis e identificación de los riesgos, continuando con la segunda subcategoría tenemos los siguientes indicadores a) Seguridad de información; b) mantenimiento y c) outsourcing.

2.4 Técnicas e instrumentos de recolección de datos

Para la recopilación de los datos se aplicó la técnica de la entrevista, la cual se define como un dialogo abierto que se establece entre dos personas, en el cual el entrevistador es el que guía al entrevistado con el objetivo de obtener información autentica acerca de un tema específico (Vargas, 2012). Por tanto, esta técnica aportó a la investigación porque permitió conocer los criterio y opiniones de los involucrados con el problema.

El instrumento aplicado fue la guía de entrevista, que está compuesta por un instrumento de recopilación de datos en donde se encuentran las dudas que tiene el entrevistador para efectuar al entrevistado, como resultado, ayuda a documentar y observar el trabajo de campo (Balcázar, González-Arratia, Gurrola, & Moysén, 2013). Por lo tanto, Sirvió de ayuda a la investigación porque se usará una entrevista como instrumento de recopilador de datos. La ficha técnica fue:

Nombre: Guía de entrevista para medir el análisis de la seguridad informática.

Autor: Martin Cristian Guevara Lunarejo

Año: 2020

Subcategorías – ítems/preguntas: SC1 Privacidad de la información (1-4); SC2 Responsabilidad en el funcionamiento de la información (5-10).

Tabla 2

Paralelo entro los instrumentos para la recopilación de datos

Subcategoría	Instrumentos Entrevista	
	Nro.	**Ítem**
Privacidad de la información	**1.**	¿Cuál es la situación del Perú con respecto a la Protección de Datos comparado con los países de la Región?
	2.	¿Por qué se conoce tan poco la ley de Habeas Data en el Perú?
	3.	¿Quién regula el análisis de la Empresa y quién identifica los riesgos de la empresa de los ataques cibernéticos?
	4.	¿Encriptas de alguna forma tus bases de datos y la información sobre tus clientes?
	5.	¿A qué se debe y qué consecuencias tiene para las empresas o entidades del estado?
	6.	¿Qué opina, cuáles son los riesgos y las ventajas de las nuevas tecnologías de comunicación?
Responsabilidad en el funcionamiento de la información	**7.**	¿Limitas el número de empleados que tienen privilegios de administrador en la infraestructura TI de tu empresa?
	8.	¿Quién es responsable de instalar y mantener el software de seguridad en tu computadora?
	9.	¿Por qué las empresas recurren al outsourcing?
	10.	¿Qué características se debe tomar en cuenta a la hora de elegir a un outsourcing?

Respecto a la tabla 2, corresponde a los instrumentos para la recopilación de datos los cuales cuenta con la subcategoría: a) privacidad de la información acuerdo con sus respectivos ítems: ¿Cuál es la situación del Perú con respecto a la Protección de Datos comparado con los países de la Región?, ¿Por qué se conoce tan poco la ley de Habeas Data en el Perú?,

¿Quién regula el análisis de la Empresa y quién identifica los riesgos de la empresa de los ataques cibernéticos?, ¿Encriptas de alguna forma tus bases de datos y la información sobre tus clientes?, ¿A qué se debe y qué consecuencias tiene para las empresas o entidades del estado?, ¿Qué opina, cuáles son los riesgos y las ventajas de las nuevas tecnologías de comunicación?; subsiguientemente con la subcategoría b) responsabilidad en el funcionamiento de la información acuerdo con sus respectivos ítems: ¿Limitas el número de empleados que tienen privilegios de administrador en la infraestructura TI de tu empresa?, ¿Quién es responsable de instalar y mantener el software de seguridad en tu computadora?, ¿Por qué las empresas recurren al outsourcing?, ¿Qué características se debe tomar en cuenta a la hora de elegir a un outsourcing?

2.5 Proceso de recolección de datos

Para la recopilación de datos, se siguió los siguientes pasos: 1) Revisión de la literatura o del marco teórico; 2) Diseño de instrumentos; 3) Recopilación de la información; 4) Aplicación de la entrevista; 5) Diseño del análisis documental; 6) Aplicación del análisis documental; 7) Triangulación; 8) Redacción del informe final.

2.6 Método de análisis de datos

Para el estudio se aplicará la triangulación, es un método de análisis de datos de proceso que busca la integración de distintos datos que permite garantizar los resultados obtenidos evidenciando una explicación más verídica de la investigación (Betrián, Galitó, García, Jové, & Macarulla, 2013). En este sentido, ayudó a la investigación porque permitió demostrar la credibilidad de los resultados de la entrevista y los datos fueron procesados en el programa Atlas. Ti 8.

2.7 Aspectos éticos

En este trabajo de investigación se utilizó la norma APA a fin de evidenciar que no incurrió en algún tipo de plagio, y que la información brindada no fue falseada.

Se solicitó la opinión de los informantes y se admitió como válida para la investigación, debido a que tienen vínculo directo con el problema.

El contenido de la data no ha sido modificado ni manipulado a fin de mostrar información veraz y fehaciente.

III. RESULTADOS

3.1 Categorización del estudio

Los resultados cualitativos obtenidos por medio de la entrevista realizada a 5 unidades informantes, cuyos cargos ocupan actualmente son: jefe de sistemas, Analista de proyectos, Mediante de esta forma, Analista de sistemas, Desarrollador, Asistente de soporte. Mediante de esta forma, se captó primeramente conocimientos necesarios e interrogantes para buscar o plantear propuesta, alternativa y soluciones.

Los resultados que se consiguieron, van a responder a nuestro objetivo general y nuestros objetivos específicos de este trabajo de investigación, por medio de las entrevistas realizadas.

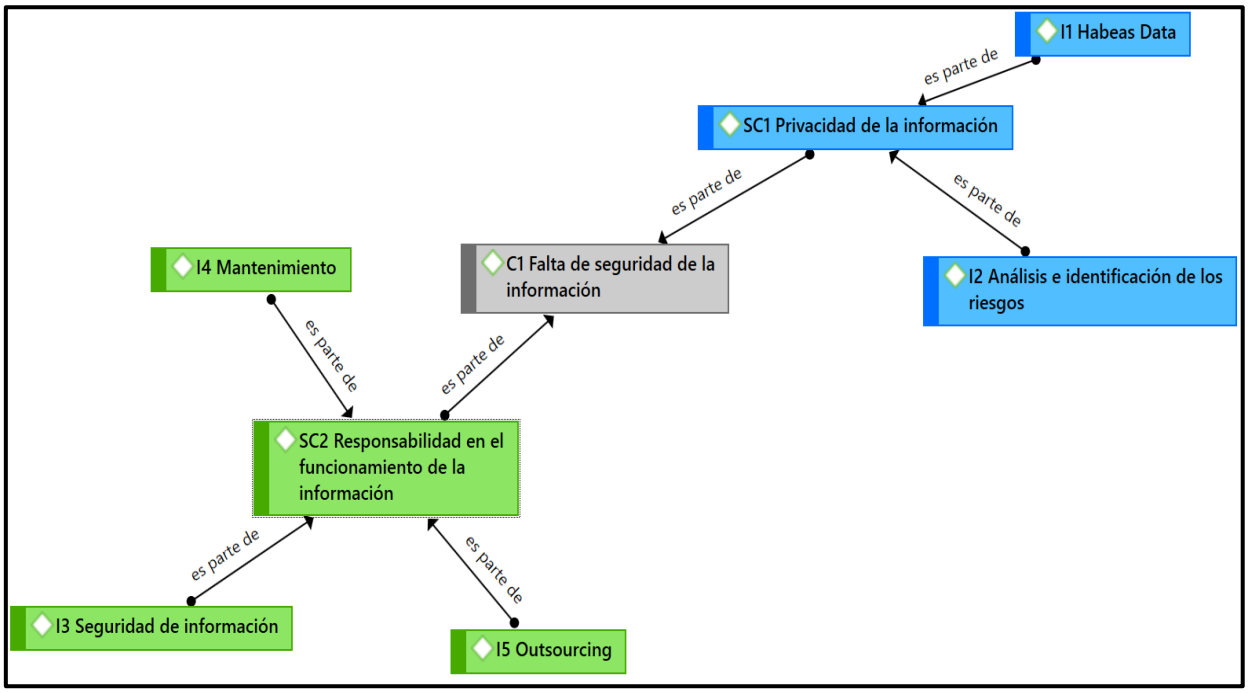


Figura 1. Matriz de categorización

En la figura 1 partimos de la variable o categoría principal que es la falta de seguridad de la información y este mismo se divide en 2 subcategorías que son: a) privacidad de la información; b) responsabilidad en el funcionamiento de la información. Posteriormente de cada subcategoría se disgrega en indicadores comenzando por la primera subcategoría a) habeas data; b) análisis e identificación de los riesgos, continuando con la segunda subcategoría tenemos los siguientes indicadores a) Seguridad de información; b) mantenimiento y c) outsourcing.

3.2 Análisis de la seguridad informática de una mediana empresa, Lima 2019-2020

Las respuestas conseguidas del análisis de estudio se determinan:

Respecto a la protección de datos o seguridad informática no se cuenta con un control, actualmente las empresas pequeñas y medianas no cuentan con un área de TI y los riesgos de un ataque cibernético son altos, además no cuentan con un sistema que ayude el control de protección de datos y no están definidos los procesos internos, asimismo no están involucradas las áreas para efectuar las tareas requeridas, el jefe de sistemas indicó que no se está aplicando los estándares de calidad como la ISO 27001 ni verificando.

Se verificó que en la empresa no se conoce la ley del Habeas Data, porque por la misma informalidad pocos hacen el seguimiento a diferencia de las grandes empresas que si toman consciencia de su información.

En la mayoria de los casos quien regula el análisis de la empresa e identifican los riesgos mayormente son tercerizados o no le dan importancia es por eso que surgen los apuros de filtración de datos, además en algunos casos el encargado de identificar los ataques cibernéticos son el área de TI.

No están establecidos las normas ISO2700 por una mala gestión de la seguridad informática, no se cuenta con un plan de trabajo para suplir este problema, no está definido cuando o qué periodo realizar un Backup teniendo así duplicidad de información.

Como resultado en muchas ocasiones, cuando el dueño solicita la información no se tiene actualizada al completó, porque no hay control de la documentación, no se controla entradas y salidas de la información, se emplea formatos de Excel como base de dato, pero no se actualiza y este queda a la intemperie para su manipulación de usuarios no correspondido por falta de encriptación informática, privilegios de administrador en la infraestructura TI de la empresa.

Se recalca con fuerza, tener un área de TI porque es una de las responsables de instalar y mantener los softwares de seguridad de las computadoras actualizadas, así evitar cualquier vulnerabilidad y sufrir cualquier ataque cibernético.

Cabe mencionar la importancia de contar con el control de seguridad informática, de mis exigencias que dispongo ante una eventualidad y continuidad del negocio, conocer las vulnerabilidades por áreas para ver el comportamiento que emplea cada usuario por el inapropiado manejo de información de la base de datos, duplicidad de información, gestionando así un software especializado y no teniendo errores de carga de información, error de datos de entradas y/o de salidas.

Figura 2. Red de objetivo general

En la figura 2 representa la triangulación red de objetivos general que parte con la categoría principal que es la falta de seguridad de la información y este se divide en 2 subcategorías que son: a) privacidad de la información; b) responsabilidad en el funcionamiento de la información. Posteriormente de cada subcategoría se disgrega en indicadores comenzando por la primera subcategoría a) habeas data; b) análisis e identificación de los riesgos, se observa que no las empresas pequeñas no cuentan y no capacitan a sus empleados sobre las leyes de la información, debido que las empresas no prefieren invertir en seguridad de su información y no se está aplicando los estándares de calidad, continuando con la segunda subcategoría tenemos los siguientes indicadores a) Seguridad de información; b) mantenimiento y c) outsourcing y se observa que no se limita los privilegios de administrador a los usuarios al instalar sus propios programas. Así mismo, en cuanto al outsourcing, se ha visto que al recurrir al outsourcing porque los costos beneficio disminuyen áreas y personal especializado. Por último, se obtuvo como fuente de información las 5 entrevistas realizadas.

Figura 3. Nube de palabras

En la figura 3 representa la nube de palabras por medio del aplicativo Atlas. Ti, que se obtuvo como fuente de información de las 5 entrevistas realizadas, podemos identificar

resultados como: información, riesgos, seguridad, privacidad, infraestructura, áreas, control, privilegios, datos, empresa, personal, TI, procesos que son palabras fuertes que resultaron de este trabajo de investigación.

3.3 Análisis de la privacidad de la información de una mediana empresa, Lima 2019-2020

Las respuestas obtenidas para los resultados de mi objetivo específico 1 son:
En la empresa no cuenta con una privacidad de la información, sin embargo, los únicos controles que se verifican, es al momento de efectuar una actualización de antivirus y al actualizar el Update del sistema operativo; asimismo, es obligatorio tener un registro de todo tratamiento que se efectúa en la información, cuando se manejan la base de datos que se clasifiquen como alto riesgo se deberá analizar y reunir todos los riesgos y prevenir filtraciones.

Según la analista de sistemas, la privacidad de la información de la empresa está en proceso porque en los últimos años no se ha tenido la mayor importancia de privacidad de esa fuente de información del usuario, debido a las múltiples quejas de los usuarios, se van a empezar a tomar acciones.

El otro control que se hace mención de los resultados de la falta de privacidad de la información al no contar con el área de TI, es quien se encarga de analizar e identificar los riesgos informáticos de la empresa, también comunicar e implementar estrategias de ciberseguridad.

Según los resultados obtenidos no hay un control de la seguridad informática, tampoco hay incremento de madurez en la gestión de la seguridad informática, para ciertas acciones de información no se realiza los cifrados simétricos y en otros asimétricos como Backup de bases de datos, aplicaciones de los sistemas y claves de accesos.

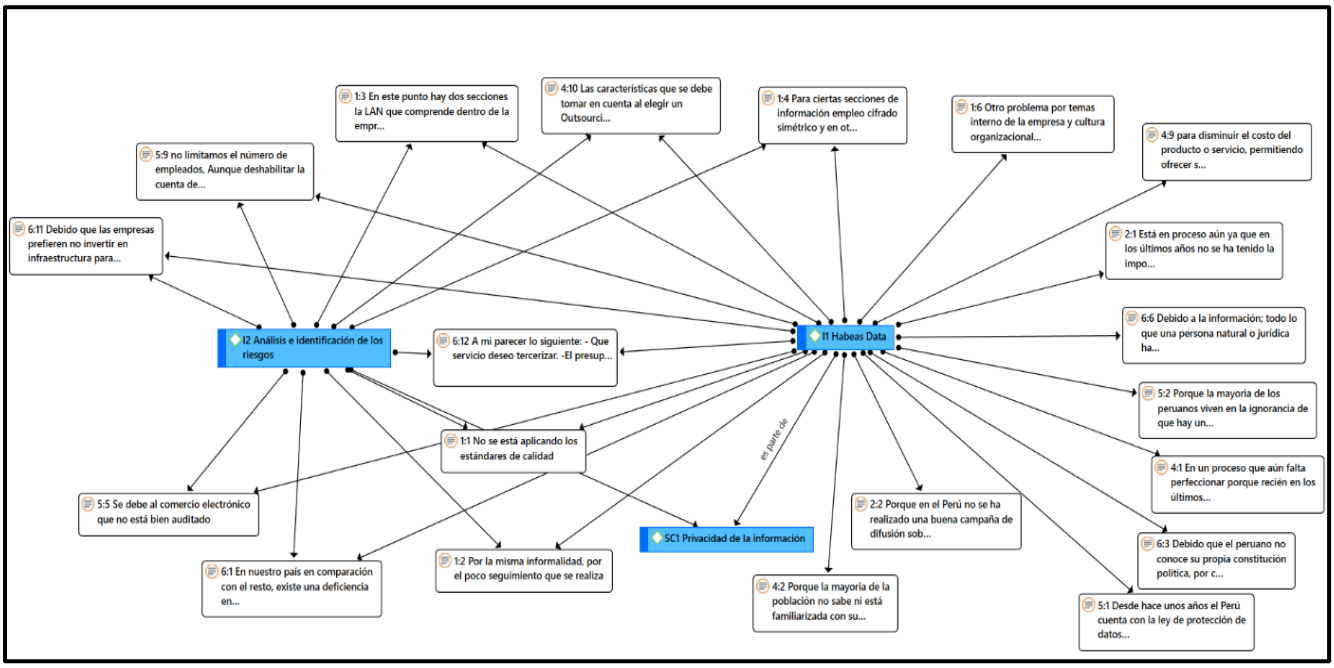


Figura 4. Red de objetivo específico 1

En la figura 4 representa la triangulación red de objetivo específico 1 por medio del aplicativo Atlas. Ti, se inicia por la subcategoría principal que es privacidad de la información, a continuación de la subcategoría se disuelve en 2 indicadores que son: a) habeas data y b) análisis e identificación de los riesgos.

Por otro lado, en el indicador habeas data se ha observado que la mayoria de la población no sabe ni está familiarizado con sus derechos de privacidad de información, debido que el peruano no conoce su propia constitución política, por consiguiente, no conoce sus derechos.

Así mismo, en el siguiente indicador análisis e identificación de los riesgos, en las empresas no se está aplicando los estándares de calidad debido a que las empresas prefieren no invertir en infraestructuras para ser administradas por ellas mismas; sino que prefieren tercerizar la infraestructura como servicio, para olvidarse de todas las actividades y gastos que se tendrían que realizar, en relación con el indicador, para tener un análisis de la empresa se identifica los riesgos por un posible ataque cibernético hay que tomar en cuenta dos punto, la lan que comprende dentro de la empresa que el área de seguridad informática en otros casos el área de soporte y redes lo realizan, establecer políticas, reglas y procedimientos. Por

otro lado, está la WAN que se encarga de los ataques a todo nuestro dominio, el tráfico de internet, descarga, visitas de páginas, etc. ellos son responsables de lo que ocurre del exterior y lo que ingresa dentro de la empresa. (virus, ransoware, protocolos).

3.4 Análisis de la responsabilidad en el funcionamiento de la información de una mediana empresa, Lima 2019-2020

Las respuestas obtenidas para los resultados de mi objetivo específico 2 son:
La responsabilidad en el funcionamiento de la información se debe a que por el conformismo de que nunca será atacado, también puede ser por poco interés de inversión en el aspecto de seguridad, otro problema es por temas internos de la empresa y cultura organizacional. La analista de sistemas indicó que cree que es por el costo de la solución para combatir ataques cibernéticos.

Las consecuencias son pérdida de información sensible y terminen en problemas legales con los clientes terminando con la reputación de la empresa. El jefe de sistemas considera lo siguiente: Se presenta una mayor motivación, interacción con la tecnología, aprenden a partir de los errores, aprendizaje colaborativo, es desarrollada la habilidad de búsqueda y selección de la información, desarrolla la expresión y la creatividad, facilidad de acceso a muchos tipos de información, el mayor riesgo es la inversión de una nueva tecnología sin haber realizado un estudio o no aplicarlo y sacarle el máximo provecho.

El riesgo de no limitar el número de empleados que tengas privilegios de administrados en la infraestructura TI es muy delicado, porque cuando un usuario le entrega privilegios de la base de datos el riesgo puede ser innecesario, puede ocurrir un abuso de privilegios de los usuarios al tener acceso a los datos legítimos para fine no permitidos. El analista de proyectos refiere que es mejor limitar los privilegios solamente para el área encargada.

Ante los resultados obtenidos, al no poder tener un control de la seguridad informática sin el área de TI, no aporta en la toma de decisiones para recurrir a un outsourcing, teniendo en cuenta las características para tomar: la seguridad, reputación, mantenimiento, costos, experiencia y garantía que se brindan

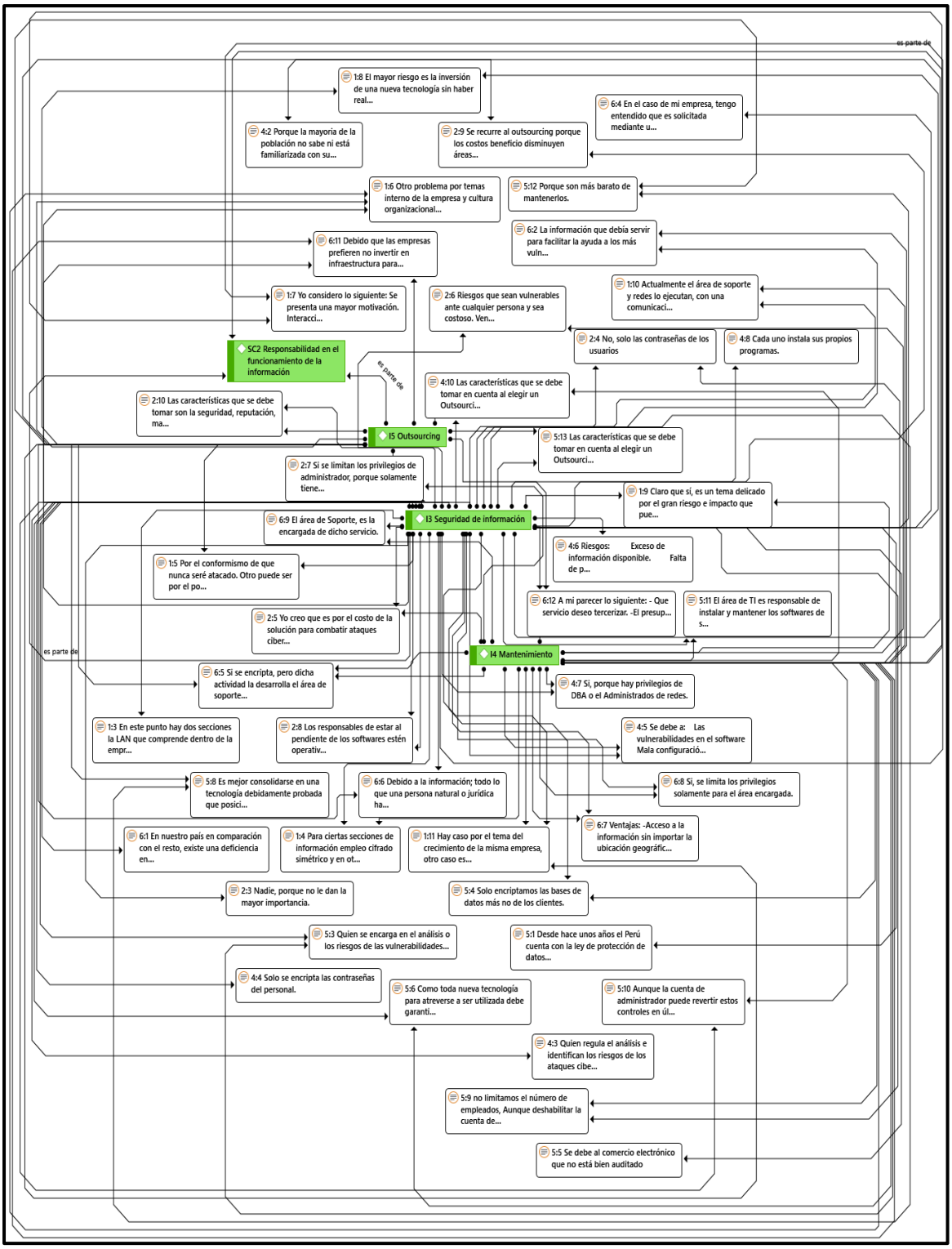


Figura 5. Red de objetivo específico 2

En la figura 5 representa la triangulación red de objetivos específicos 2 por medio del aplicativo Atlas. Ti, se encabeza por la subcategoría principal la cual es la responsabilidad en el funcionamiento de la información, posteriormente de la subcategoría se disgrega en 3

indicadores que son: a) seguridad de información; b) mantenimiento y c) outsourcing se observan que la seguridad de información, el área de TI es responsable de instalar, mantener los softwares de seguridad activas en las computadoras, no contar con una mala configuración de los sistemas, malos hábitos de seguridad, y sus consecuencias son: perdida de información confidencial, interrupción de las operaciones. En cuanto a seguridad de información, en nuestro país existe una deficiencia en infraestructura de TI y gobierno de información, se observa en lo ocurrido en la cuarentena, debido que el estado no cuenta con la totalidad de información del ciudadano, por diversos factores.

Respecto al indicador mantenimiento, los entrevistados indican que, para ciertas secciones de información se emplea el cifrado simétrico y en otros asimétrico como Backup de base de datos, aplicaciones de los sistemas, claves de accesos, asimismo el área de ti se encarga de dar los privilegios de acceso para dicha encriptación.

Por otro lado, con el indicador outsourcing, se indica que hay caso por el tema del crecimiento de la misma empresa, otro caso es para tener todo alineado, si es cierto la gestión y control de los activos del área de TI es complejo, como mantenimiento de equipos, impresoras, control de servidores, licenciamiento, toma de inventario de activo fijo, tiempo de respuesta para cambios de repuestos de los equipos y que no exista control de entradas y salidas. El outsourcing facilita esa tarea con software de control para distintos escenarios, y como se debe tomar en cuenta a la hora de elegir a un outsourcing son: ¿qué tipo de subcontratación se está buscando?,¿qué es lo que se desea externalizar? ¿Cuáles son las ubicaciones de offshore outsourcing que te interesa?, ¿cuánto planeas gastar?, ¿cuáles son los riesgos?, ¿cuáles son sus referencias de otras empresas? Y así disminuir el costo del producto servicio, permitiendo ofrecer servicios de alta calidad buscando maximizar sus operaciones y minimizar los riesgos.

IV. DISCUSIÓN, CONCLUSIONES Y RECOMENDACIONES

4.1 Discusión

Respectos a mis antecedentes internacionales, coincido con Knorst, Vanti, Espín Andrade, Silvio (2011), evidenciaron que es posible establecer una relación utilizando estratégicamente los criterios de seguridad e integrarlos a través del modelo BSC, COBIT e ISO27002 ya que estos facilitan el mapeo de objeticos genéricos para el negocio de TI desde la perspectiva del BSC con los objetivos generales de TI. Al mismo tiempo, se coincide con Allassani (2014), porque constata que la mayoría del personal no tiene buenos hábitos de lectura sobre las políticas de seguridad de la empresa, Los empleados que han trabajado menos de 5 años tienen menos probabilidades de leer, incluso si son personas mayores, los ejecutivos están involucrados en el proceso de monitoreo, en base que los empleados al no tener buenos hábitos de lectura, se desea recomendar que a los empleados sean evaluados anualmente y ser recompensados.

De la misma manera, se coincide con Roratto, Dotto Dias (2014), los cuales señalaron que se presenta la importancia de garantizar la seguridad, inviolabilidad e integridad de la información contenida en un sistema de gestión informatizado, se concluye que, con la creciente dependencia de los sistemas críticos de almacenamiento de datos, desarrollar nuevas soluciones para el monitoreo y protección de estos datos y desarrollar nuevas soluciones para el monitoreo y protección de estos datos, está claro que esta es un área de estudio muy prometedora e importante, y se recomienda realizar nuevas investigaciones en el área de control y seguridad de la información a través del uso de las tecnologías de BI.

De esta forma, coinciden con Reyes Mena, Fuertes Díaz, Guzmán Jaramillo. (2017), se diseñó una solución implementada a través de Business Intelligence que actúa como un factor estratégico en el análisis de vulnerabilidad de un CSIRT y esto fue esto fue posible aplicando la metodología de Investigación-Acción y las fases de Ralph Kimball. Asimismo, coincido con Stanley Ndungu, Kenneth Wanjau, Robert Gichira, Waweru Mwangi (2017). Que evidenciaron que el estudio sobre la Teoría integrada del sistema de gestión de la seguridad de la información, identificaron la evaluación de riesgos de seguridad de la información como uno de los factores de éxito de la gestión de la seguridad de la información.

Respectos a mis antecedentes nacionales, se coincide con Cruz & Fukusaki (2017), puesto que un Sistema de Gestión de Seguridad de la Información puede ser implementada a diversas empresas sin tomar importancia al tamaño o rubro en el que se desempeñe, asimismo identificaron distintos métodos para reducir los riesgos que se presenten en las organizaciones, entre estos existen los mapeos de riesgos, declaración de aplicabilidad y la implementación de controles. Adicionalmente coincido con Lavado (2019), porque evidenció que la banca es uno de los sectores económicos que más importancia debe darle a la seguridad informática. Esto se debe a que el banco ya tiene implementado otros estándares como la ISO/IEC 27001 y ley de protección de datos (Ley N° 29733), los cuales coinciden con algunos requerimientos de la norma PCI DSS. Por lo que este estándar no reemplaza, los ya implementados, si no, los complementa para darle más seguridad a la organización. Además, Fernández & Pacheco (2014), acreditan que el resultado es minimizar los riesgos, amenazas y vulnerabilidades de los activos de información como también el compromiso del personal de la Comandancia con respecto a la seguridad de información. De esta forma, se coincide con Contreras & Vega (2019), puesto que demostraron que se presenta la planificación que garantiza el correcto funcionamiento de la solución Privileged Access Manager. La cual permite disminuir el riesgo interno de seguridad informática con los activos de TI y tiene la trazabilidad de todas las actividades realizadas por los administradores del área de redes, seguridad y base de datos de la empresa, del mismo modo coincido con Chauca Huaman (2017), porque demostró que la propuesta de un aplicativo web para la gestión de las auditorías informáticas para la empresa Calzado Atlas S.A. es viable luego del análisis económico, análisis de ahorro en gasto de incidentes del área de TI y análisis de rentabilidad, como solución informática para la necesidad que presenta.

4.2 Conclusiones

Primera **:** Se efectuó una investigación donde se utilizó la entrevista para obtener información, de igual manera se identificó que la empresa no cuenta con área de TI que se requiere para un mejor control sobre la seguridad de información, no se cuenta con ningún procedimiento manual ni sistémica hacia la protección de datos, del mismo modo la empresa no tiene conocimiento sobre la ley Habeas Data por falta de cultura de la informalidad. La gestión administrativa no es lo bastante colaborativa, la determinación de la existencia de la data no se tiene actualizada, los procesos no están bien definidos, bajo este punto no se cuenta con una gestión y planeación correcta del control de la base de datos de una mediana empresa para un mejor control de seguridad informática.

Segunda **:** En cuanto al objetivo específico la privacidad de la información de la empresa, no cuenta con una privacidad informática especializada, no obstante, los únicos controles que se maneja en la empresa son las actualizaciones del Update y antivirus, la empresa no cuenta con la madurez para la gestión de la seguridad informática para ciertas acciones informáticas, no se realizan las encriptaciones simétricos y asimétricos, asimismo se ha empezado a darle importancia a la privacidad de información del usuario porque los mismos usuarios han identificado las vulnerabilidades de la base de datos.

Tercera **:** En relación respecto al análisis de la responsabilidad en el funcionamiento de la información, no se cuenta con un análisis adecuado por el mismo conformismo de creer que nunca serán atacados, se ve poco el interés de invertir en la infraestructura de la seguridad informática. Adicionalmente, las consecuencias son graves, porque se habla de pérdida de información y terminen en problemas legales con la empresa. Por otra parte, no se limita el número de empleados con los privilegios de administrador en la infraestructura de TI, al darle privilegios administrativos a los usuarios es muy delicado porque se puede usar los datos de la empresa, base de datos de la empresa en forma ilícita. Para concluir ante los resultados obtenidos. Al no

contar con un área de TI es difícil tener un control general sobre la seguridad informática de la empresa y sin contar con un outsourcing especializado.

4.3 Recomendaciones

Primera **:** Se recomienda incluir las políticas institucionales la seguridad informática de tecnología ampliando normas e involucrando un área de TI para un mejor control sobre la seguridad informática, contar con un procedimiento manual o sistemático hacia la protección de datos, incentivar a los usuarios a tener conocimiento sobre las leyes que nos ampara como el Habeas Data. Asimismo, tener involucradas todas las áreas intervenidas de esta investigación, de tal manera que la data sea unificada y actualizada, teniendo así los procesos bien definidos con una buena gestión y planificación para un control de la base de datos de la empresa llevando así un registro de ocurrencias de los riesgos.

Segunda **:** Respecto a la privacidad de la información se recomienda tener en cuenta que los ataques cibernéticos son por medio DoS/DDoS que son utilizados para interrumpir los servicios de la empresa, secuestro de data por medio de Malwares, por eso es tener una madurez en la empresa para poder hacer un análisis sobre los riesgos que se puedan perpetuar y tener acciones inmediatas, las acciones que se deben que tomar son las encriptaciones simétricas e asimétricas como Backup de base de datos, aplicaciones de los sistemas, claves de accesos.

Tercera **:** En cuanto respecto al análisis de la responsabilidad en el funcionamiento de la información, se debe contar con un análisis adecuado para estar siempre alerta sobre algún ataque cibernético o alguna vulnerabilidad en la infraestructura de la seguridad informática, así mismo no haya duplicidad o perdida de información. Asimismo, limitar el privilegio de administrador a los usuarios y sea únicamente privilegiado el personal del área de TI.

REFERENCIAS

Akhtar, I. (2016). Research in Social Science: Interdisciplinary Perspectives. *Research in Social Science: Interdisciplinary Perspectives* , 68-84.

Álvarez, E., Carreño, S., Tirado, N., & Ramos, D. (2017). Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas. *Revista Publicando, 4*(10, 2), 462-473. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=6115230

Balcázar, P., González-Arratia, N., Gurrola, G., & Moysén, A. (2013). *Investigación cualitativa.* Ciudad de México: Universidad Autónoma del Estado de México. Obtenido de http://repositorio.minedu.gob.pe/handle/123456789/4641

Betrián, E., Galitó, N., García, N., Jové, G., & Macarulla, M. (2013). La triangulación múltiple como estrategia metodológica. *Revista Iberoamericana sobre Calidad, Eficacia y Cambio en Educación, 11*(4), 5-24. Obtenido de https://www.redalyc.org/pdf/551/55128238001.pdf

Clausó, A. (1993). Análisis documental: el análisis formal. *Revista General de Información y Documentación, 3*(1), 11-19.

Díaz, O., & Muñoz, M. (Marzo de 2018). Implementación de un enfoque DevSecOps + Risk Management en un Centro de Datos de una organización Mexicana. (26). doi:10.17013/risti.26.43–53

Fazlollah, Reza;. (1994). *AN INTRODUCTION TO INFORMATION THEORY.* Nueva York, Estados Unidos: DOVER PUBLICATIONS, INC. Obtenido de https://dialnet.unirioja.es/servlet/libro?codigo=370603

Gil, V., & Gil, J. (Junio de 2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *22*(2), 196-200. doi:10.22517/23447214.11371

Gomez, S. (2012). *Metodología de la Investigación* (1° ed.). Estado de México: Red Tercer Milenio. Obtenido de http://www.aliat.org.mx/BibliotecasDigitales/Axiologicas/Metodologia_de_la_investigacion.pdf

Gordón, D., & Pacheco, R. (Mayo-Octubre de 2018). Análisis de Estrategias de Gestión de Seguridad Informática con Base en la Metodología Open Source Security Testing Methodology Manual (OSSTMM) para la Intranet de una Institución de Educación Superior. *ReCIBE. Revista electrónica de Computación, Informática,, 7*(1), 1-21. Obtenido de https://www.redalyc.org/jatsRepo/5122/512255650001/index.html

Gregorio, C., & Ornelas, L. (2011). *Protección de Datos personales en las Redes Sociales Digitales: en particular de niños y adolecentes.* D.F., México. Obtenido de https://archivos.juridicas.unam.mx/www/bjv/libros/12/5667/13.pdf

Herbert, S. (1997). *Administrative Behavior.* Nueva York: The Free Press. Obtenido de https://catalogo.rebiun.org/rebiun/doc?q=0-684-83582-7+%7C%7C+0684835827&start=0&rows=1&sort=score%20desc&fq=msstored_mlt172&fv=LIB&fo=and&redo_advanced=false

Hernández, R., Fernández, C., & Baptista, M. (2014). *Metodología de la Investigación.* Ciudad de México: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V. Obtenido de http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdf

Luhmann, N. (1996). *Introducción a la teoría de sistemas.* Universidad Iberoamericana. Obtenido de https://libgen.pw/links?id=2273467

Muñoz, M., & Rivas, L. (Marzo de 2015). Estado actual de equipos de respuesta a incidentes de seguridad informática. *Revista Ibérica de Sistemas e Tecnologias de Información*(3). Obtenido de http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952015000100002

Peterson, M. (2009). *An Introduction to Decision Theory.* Cambridge University Press. doi:https://doi.org/10.1017/CBO9780511800917

Proaño, R., & Gavilanes, A. (Marzo de 2018). Estrategia para responder a incidentes de inseguridad informática ambientado en la legalidad ecuatoriana. *Enfoque UTE*, 90-101. doi:10.29019/enfoqueute.v9n1.229

Rojas, R. (2013). *Guía para realizar investigaciones sociales.* Ciudad de México: Plaza y Valdés S. A. Obtenido de https://raulrojassoriano.com/cuallitlanezi/wp-content/themes/raulrojassoriano/assets/libros/guia-realizar-investigaciones-sociales-rojas-soriano.pdf

Romero, A. (27 de Septiembre de 2017). Privacidad e Intimidad en las Redes Sociales. *Universidad Internacional de La Rioja*, 2-73. Obtenido de https://reunir.unir.net/bitstream/handle/123456789/6637/ROMERO%20ROBREDO%2C%20ANDREA.pdf?sequence=1&isAllowed=y

Shannon, C., & Warren, W. (1948). *THE MATHEMATICAL THEORY OF COMMUNICATION* (Vol. 27). THE BELL SYSTEM TECHNICAL JOURNAL. Obtenido de http://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf

Solís, F., Pinto, D., & Solís, S. (2017). Seguridad de la información en el intercambio de datos entre dispositivos. *Enfoque UTE, 8*(1), 160-171. doi:10.29019/enfoqueute.v8n1.123

Soto, Y. (Julio de 2017). Datos masivos con privacidad y no contra privacidad. *Revista de Bioética y Derecho*(40), 101-114. Obtenido de https://www.redalyc.org/pdf/783/78351101008.pdf

Stake, R. (1999). *Investigación con estudio de casos.* Madrid: Ediciones Morata S.L. Obtenido de https://www.uv.mx/rmipe/files/2017/02/Investigacion-con-estudios-de-caso.pdf

Tarazona, C. (2007). AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN. *28*(84), 137- 146. Obtenido de https://revistas.uexternado.edu.co/index.php/derpen/article/view/965

Vargas, I. (2012). LA ENTREVISTA EN LA INVESTIGACIÓN CUALITATIVA: NUEVAS TENDENCIAS Y RETOS. *Revista Calidad en la Educación Superior, 3*(1), 119-139. Obtenido de http://biblioteca.icap.ac.cr/BLIVI/COLECCION_UNPAN/BOL_DICIEMBRE_2013_69/UNED/2012/investigacion_cualitativa.pdf

Von Bertalanffy, L. (1976). *GENERAL SYSTEMS THEORY; Fundamentals, development, applications.* México: Fondo de Cultura Económica. Obtenido de https://cienciasyparadigmas.files.wordpress.com/2012/06/teoria-general-de-los-sistemas-_-fundamentos-desarrollo-aplicacionesludwig-von-bertalanffy.pdf

ANEXOS

Anexo 1: Matriz de la investigación

Título: Análisis de la seguridad informática de una mediana empresa, Lima 2019-2020

<table>
<tr><td rowspan="2">Problema general</td><td rowspan="2">Objetivo general</td><td colspan="3">Categoría 1:</td></tr>
<tr><td>Sub categorías</td><td>Indicadores</td><td>Ítem</td></tr>
<tr><td rowspan="4">¿Cuál es la situación de la seguridad informática de una mediana empresa, Lima 2019-2020?</td><td rowspan="4">Analizar la seguridad informática de una mediana empresa, Lima 2019-2020</td><td rowspan="4">SC1Privacidad de la información</td><td rowspan="2">I1Habeas Data</td><td>1. Cuál es la situación del Perú con respecto a la Protección de Datos comparado con los países de la Región?</td></tr>
<tr><td>2. ¿Por qué se conoce tan poco la ley de Habeas Data en el Perú?</td></tr>
<tr><td rowspan="2">I2Análisis e identificación de los riesgos</td><td>3. ¿Quién regula el análisis de la Empresa y quién identifica los riesgos de la empresa de los ataques cibernéticos?</td></tr>
<tr><td>4. ¿Encriptas de alguna forma tus bases de datos y la información sobre tus clientes?</td></tr>
<tr><td>Problemas específicos</td><td>Objetivos específicos</td><td rowspan="5">SC2Responsabilidad en el funcionamiento de la información</td><td rowspan="2">I3Seguridad de información</td><td>5. ¿A qué se debe y qué consecuencias tiene para las empresas o entidades del estado?</td></tr>
<tr><td>¿Cuál es la situación de la privacidad de la información de una mediana empresa, Lima 2019-2020?</td><td>Analizar la privacidad de la información de una mediana empresa, Lima 2019-2020</td><td>6. Qué opina, ¿cuáles son los riesgos y las ventajas de las nuevas tecnologías de comunicación?</td></tr>
<tr><td rowspan="2">I4Mantenimiento</td><td>7. ¿Limitas el número de empleados que tienen privilegios de administrador en la infraestructura TI de tu empresa?</td></tr>
<tr><td>¿Cuál es la situación de la responsabilidad en el funcionamiento de la información de una mediana empresa, Lima 2019-2020?</td><td>Analizar la responsabilidad en el funcionamiento de la información de una mediana empresa, Lima 2019-2020</td><td>8. ¿Quién es responsable de instalar y mantener el software de seguridad en tu computadora?</td></tr>
<tr><td rowspan="2">I5Outsourcing</td><td>9. ¿Por qué las empresas recurren al outsourcing?</td></tr>
<tr><td>10. ¿Qué características se debe tomar en cuenta a la hora de elegir a un outsourcing?</td></tr>
<tr><td>Método</td><td colspan="2">Población, muestra y unidad informante</td><td>Técnicas e instrumentos</td><td>Procedimiento y análisis de datos</td></tr>
<tr><td>Enfoque: Cualitativo
Método: Estudio de caso y Analítico</td><td colspan="2">Unidad informante:
✓ Victor Ramírez
✓ Dianeth Lizárraga,
✓ Francisco Acaro
✓ Jordy Llanos
✓ Arturo Aquino</td><td>Técnicas: Entrevista
Instrumentos: Guía de entrevista</td><td>Procedimiento: recopilar artículos, revistas, libros, tesis.
Análisis de datos: Atlas.ti</td></tr>
</table>

Anexo 2: Instrumento cualitativo

Entrevistado # - Nombre y Apellido

Fecha: **/**/****

Hora: **:**:**

---

1. ¿Cuál es la situación del Perú con respecto a la Protección de Datos comparado con los países de la Región?

2. ¿Por qué se conoce tan poco la ley de Habeas Data en el Perú?

3. ¿Quién regula el análisis de la Empresa y quién identifica los riesgos de la empresa de los ataques cibernéticos?

4. ¿Encriptas de alguna forma tus bases de datos y la información sobre tus clientes?

5. ¿A qué se debe y qué consecuencias tiene para las empresas o entidades del estado?

6. ¿Qué opina, cuáles son los riesgos y las ventajas de las nuevas tecnologías de comunicación?

7. ¿Limitas el número de empleados que tienen privilegios de administrador en la infraestructura TI de tu empresa?

8. ¿Quién es responsable de instalar y mantener el software de seguridad en tu computadora?

9. ¿Por qué las empresas recurren al outsourcing?

10. ¿Qué características se debe tomar en cuenta a la hora de elegir a un outsourcing?

Anexo 3: Transcripción de las entrevistas o informe del análisis documental

Entrevistado 1- VICTOR NOE RAMIREZ PALOMINO

Fecha: 11/06/2020

Hora: 19:26:42

---

1. ¿Cuál es la situación del Perú con respecto a la Protección de Datos comparado con los países de la Región?

   No se está aplicando los estándares de calidad como la ISO 27001 ni verificando.

2. ¿Por qué se conoce tan poco la ley de Habeas Data en el Perú? .

Por la misma informalidad, por el poco seguimiento que se realiza sobre todo a las grandes empresas.

3. ¿Quién regula el análisis de la Empresa y quién identifica los riesgos de la empresa de los ataques cibernéticos?

En este punto hay dos secciones la LAN que comprende dentro de la empresa que el área de seguridad informática en otros casos el área de soporte y redes lo realizan, establecer políticas, reglas y procedimientos. Por otro lado, está la WAN que se encarga de los ataques a todo nuestro dominio, el tráfico de internet, descarga, visitas de páginas, etc. ellos son responsables de lo que ocurre del exterior y lo que ingresa dentro de la empresa. (Virus, RANSOWARE, PROTOCOLOS).

4. ¿Encriptas de alguna forma tus bases de datos y la información sobre tus clientes?

Para ciertas secciones de información empleo cifrado simétrico y en otros asimétrico (como Backup de base de datos, aplicaciones de los sistemas, claves de accesos)

5. ¿A qué se debe y qué consecuencias tiene para las empresas o entidades del estado?

Por el conformismo de que nunca seré atacado. Otro puede ser por el poco interés de inversión en el aspecto de seguridad. Otro problema por temas interno de la empresa y cultura organizacional.

6. ¿Qué opina, cuáles son los riesgos y las ventajas de las nuevas tecnologías de comunicación?

"Yo considero lo siguiente:
Se presenta una mayor motivación.
Interacción con la tecnología.
Aprenden a partir de los errores.
Aprendizaje colaborativo.
Es desarrollada la habilidad de búsqueda y selección de la información.
Desarrolla la expresión y la creatividad.
Facilidad de acceso a muchos tipos de información.
El mayor riesgo es la inversión de una nueva tecnología sin haber realizado un estudio o no aplicarlo y sacarle el máximo provecho."

7. ¿Limitas el número de empleados que tienen privilegios de administrador en la infraestructura TI de tu empresa?

Claro que sí, es un tema delicado por el gran riesgo e impacto que pueda ocurrir. A eso hay que acompañar el nivel de confianza que la Gerencia otorgue a la persona asignada que a su vez también es una gran responsabilidad. Actualmente está limitado sólo a 3 personas.

8. ¿Quién es responsable de instalar y mantener el software de seguridad en tu computadora?

Actualmente el área de soporte y redes lo ejecutan, con una comunicación al Jefe de Sistema y a la Gerencia.

9. ¿Por qué las empresas recurren al outsourcing?

Hay caso por el tema del crecimiento de la misma empresa, otro caso es para tener todo alineado, si es cierto la gestión y control de los activos del área de TI es complejo, como mantenimiento de equipos, impresoras, control de servidores, licenciamiento, toma de inventario de activo fijo, tiempo de respuesta para cambios de repuestos de los equipos y que no exista control de entradas y salidas. El outsourcing facilita esa tarea con software de control para distintos escenarios.

10. ¿Qué características se debe tomar en cuenta a la hora de elegir a un outsourcing?

Para definir se tendría que responder a estas preguntas en función de ello se puede tomar una decisión siempre es recomendable comparar y tener más de una opción.
¿Qué tipo de subcontratación se está buscando?
¿Qué es lo que se desea externalizar?
¿Cuáles son las ubicaciones de offshore outsourcing que te interesa?
¿Cuáles son tus objetivos en un outsourcing?
¿Cuánto planeas gastar?
¿Cuáles son los riesgos?
¿Cuáles son sus referencias de otra empresas?
Lo legible en el tema del contrato.

Entrevistado 2 - Dianeth Lizarraga Meza

Fecha: 11/06/2020

Hora: 23:55:50

1. ¿Cuál es la situación del Perú con respecto a la Protección de Datos comparado con los países de la Región?

Está en proceso aún ya que en los últimos años no se ha tenido la importancia de esa fuente de información del usuario, debido a las múltiples quejas de los usuarios se han empezado a tomar acciones. Perú comparado con otros países está en el 1%.

2. ¿Por qué se conoce tan poco la ley de Habeas Data en el Perú?

Porque en el Perú no se ha realizado una buena campaña de difusión sobre el Habeas Data.

3. ¿Quién regula el análisis de la Empresa y quién identifica los riesgos de la empresa de los ataques cibernéticos?

Nadie, porque no le dan la mayor importancia.

4. ¿Encriptas de alguna forma tus bases de datos y la información sobre tus clientes?

No, solo las contraseñas de los usuarios

5. ¿A qué se debe y qué consecuencias tiene para las empresas o entidades del estado?

Yo creo que es por el costo de la solución para combatir ataques cibernéticos. Las consecuencias son pérdida de información sensible y termine en problemas legales con los clientes terminando con la reputación de la empresa

6. ¿Qué opina, cuáles son los riesgos y las ventajas de las nuevas tecnologías de comunicación?

Riesgos que sean vulnerables ante cualquier persona y sea costoso. Ventajas que pueda ayudar a optimizar procesos minimizando riesgos.

7. ¿Limitas el número de empleados que tienen privilegios de administrador en la infraestructura TI de tu empresa?

Si se limitan los privilegios de administrador, porque solamente tiene el privilegio el encargado de área.

8. ¿Quién es responsable de instalar y mantener el software de seguridad en tu computadora?

Los responsables de estar al pendiente de los softwares estén operativos son el jefe de sistemas y yo.

9. ¿Por qué las empresas recurren al outsourcing?

Se recurre al outsourcing porque los costos beneficio disminuyen áreas y personal especializado.

10. ¿Qué características se debe tomar en cuenta a la hora de elegir a un outsourcing?

Las características que se debe tomar son la seguridad, reputación, mantenimiento y costos.

Entrevistado 3 - Francisco Acaro León

Fecha: 14/06/2020

Hora: 19:31:22

---

1. ¿Cuál es la situación del Perú con respecto a la Protección de Datos comparado con los países de la Región?

En nuestro país en comparación con el resto, existe una deficiencia en Infraestructura de TI y gobierno de la información, el reflejo de lo mencionado se puede observar en lo ocurrido en la cuarentena. Debido que el Estado no cuenta con la totalidad de información del ciudadano, por diversos factores. La información que debía servir para facilitar la ayuda a los más vulnerables, fue en muchos casos dirigida y robada, para fines personales.

2. ¿Por qué se conoce tan poco la ley de Habeas Data en el Perú?

Debido que el peruano no conoce su propia constitución política, por consiguiente, no conoce sus propios derechos.

3. ¿Quién regula el análisis de la Empresa y quién identifica los riesgos de la empresa de los ataques cibernéticos?

En el caso de mi empresa, tengo entendido que es solicitada mediante una prestación de servicios, porque es tercerizado.

4. ¿Encriptas de alguna forma tus bases de datos y la información sobre tus clientes?

Si se encripta, pero dicha actividad la desarrolla el área de soporte donde trabajo.

5. ¿A qué se debe y qué consecuencias tiene para las empresas o entidades del estado?

Debido a la información; todo lo que una persona natural o jurídica hace es registrada sus datos (médicos, su identidad, estados financieros). Como consecuencia las empresas bancarias y del estado sufren ataques para obtener dicha información y poder ser utilizada con fines lucrativos, delincuenciales, etc.

6. ¿Qué opina, cuáles son los riesgos y las ventajas de las nuevas tecnologías de comunicación?

Ventajas:
-Acceso a la información sin importar la ubicación geográfica.
-Optimizan los recursos humanos y económicos.
- Interconectividad sin límites.
-Aumento de la productividad.

Riesgos:
- Potenciales ataques cibernéticos.
- Robo de información a una empresa.

7. ¿Limitas el número de empleados que tienen privilegios de administrador en la infraestructura TI de tu empresa?

Si, se limita los privilegios solamente para el área encargada.

8. ¿Quién es responsable de instalar y mantener el software de seguridad en tu computadora?

El área de Soporte, es la encargada de dicho servicio.

9. ¿Por qué las empresas recurren al outsourcing?

Debido que las empresas prefieren no invertir en infraestructura para ser administradas por ellas mismas; sino que prefieren tercerizar la infraestructura como servicio, para olvidarse de todas las actividades y gastos que se tendría que realizar.

10. ¿Qué características se debe tomar en cuenta a la hora de elegir a un outsourcing?

A mi parecer lo siguiente:
- Que servicio deseo tercerizar.
-El presupuesto disponible para dicho servicio.
-Experiencia y valoración en efectividad del outsourcing
- Soluciones tecnológicas que ofrecen para dicha actividad

Entrevistado 4 - Jordy Llanos Becerra

Fecha: 16/06/2020

Hora: 19:47:57

---

1. ¿Cuál es la situación del Perú con respecto a la Protección de Datos comparado con los países de la Región?

En un proceso que aún falta perfeccionar porque recién en los últimos años se está viviendo una transformación digital en nuestro país.

2. ¿Por qué se conoce tan poco la ley de Habeas Data en el Perú?

Porque la mayoria de la población no sabe ni está familiarizada con sus derechos de privacidad de información

3. ¿Quién regula el análisis de la Empresa y quién identifica los riesgos de la empresa de los ataques cibernéticos?

Quien regula el análisis e identifican los riesgos de los ataques cibernéticos de la empresa son el área de TI

4. ¿Encriptas de alguna forma tus bases de datos y la información sobre tus clientes?

Solo se encripta las contraseñas del personal.

5. ¿A qué se debe y qué consecuencias tiene para las empresas o entidades del estado?

Se debe a:
- Las vulnerabilidades en el software
- Mala configuración de los sistemas
- Malos hábitos de seguridad

Consecuencias.
- Perdidas de información confidencial
- Interrupción de las operaciones

6. ¿Qué opina, cuáles son los riesgos y las ventajas de las nuevas tecnologías de comunicación?

Riesgos:
- Exceso de información disponible.
- Falta de privacidad y uso indebido de datos personales.
- Suplantación de la identidad
- Contacto con desconocidos
- Información inapropiada.

Ventajas:
- Mejoran la comunicación
- Permiten manejar y disponer de todo tipo de información.
- Nuevas formas de aprendizaje.

7. ¿Limitas el número de empleados que tienen privilegios de administrador en la infraestructura TI de tu empresa?

Si, porque hay privilegios de DBA o el Administrados de redes.

8. ¿Quién es responsable de instalar y mantener el software de seguridad en tu computadora?

Cada uno instala sus propios programas.

9. ¿Por qué las empresas recurren al outsourcing?

para disminuir el costo del producto o servicio, permitiendo ofrecer servicios de alta calidad, buscando maximizar sus operaciones y minimizar los riesgos

10. ¿Qué características se debe tomar en cuenta a la hora de elegir a un outsourcing?

Las características que se debe tomar en cuenta al elegir un Outsourcing es establecer con claridad las responsabilidades que tienen ambas partes en cualquier aspecto.

Entrevistado 5 - Arturo Aquino

Fecha: 16/06/2020

Hora: 23:23:04

---

1. ¿Cuál es la situación del Perú con respecto a la Protección de Datos comparado con los países de la Región?

Desde hace unos años el Perú cuenta con la ley de protección de datos que recopilan de información de carácter personal

2. ¿Por qué se conoce tan poco la ley de Habeas Data en el Perú?

Porque la mayoria de los peruanos viven en la ignorancia de que hay una ley que los ampara sobre su derecho a la privacidad en forma personal y publica

3. ¿Quién regula el análisis de la Empresa y quién identifica los riesgos de la empresa de los ataques cibernéticos?

Quien se encarga en el análisis o los riesgos de las vulnerabilidades de la empresa son del área de TI

4. ¿Encriptas de alguna forma tus bases de datos y la información sobre tus clientes?

Solo encriptamos las bases de datos más no de los clientes.

5. ¿A qué se debe y qué consecuencias tiene para las empresas o entidades del estado?

Se debe al comercio electrónico que no está bien auditado

6. ¿Qué opina, cuáles son los riesgos y las ventajas de las nuevas tecnologías de comunicación?

Como toda nueva tecnología para atreverse a ser utilizada debe garantizar su confiabilidad y esto se logra teniendo el benchmarking de otras experiencias al respecto, ya que muchas nuevas tecnologías que pretendían ser auspiciosas, quedaron en el tintero por diversas vulnerabilidades. Es mejor consolidarse en una tecnología debidamente probada que posicionarse con una nueva que no ofrezca ninguna garantía.

7. ¿Limitas el número de empleados que tienen privilegios de administrador en la infraestructura TI de tu empresa?

no limitamos el número de empleados, Aunque deshabilitar la cuenta de administrador en un dominio hace que la cuenta sea inutilizable, debe implementar restricciones adicionales en la cuenta en caso de que la cuenta esté habilitada de forma inadvertida o malintencionada. Aunque la cuenta de

administrador puede revertir estos controles en última instancia, el objetivo es crear controles que ralenticen el progreso de un atacante y limitar el daño que puede infligir la cuenta

8. ¿Quién es responsable de instalar y mantener el software de seguridad en tu computadora?

El área de TI es responsable de instalar y mantener los softwares de seguridad activas en las computadoras

9. ¿Por qué las empresas recurren al outsourcing?

Porque son más barato de mantenerlos.

10. ¿Qué características se debe tomar en cuenta a la hora de elegir a un outsourcing?

Las características que se debe tomar en cuenta al elegir un Outsourcing es experiencia y garantía que se brindan.

Anexo 4: Pantallazos del Atlas.ti

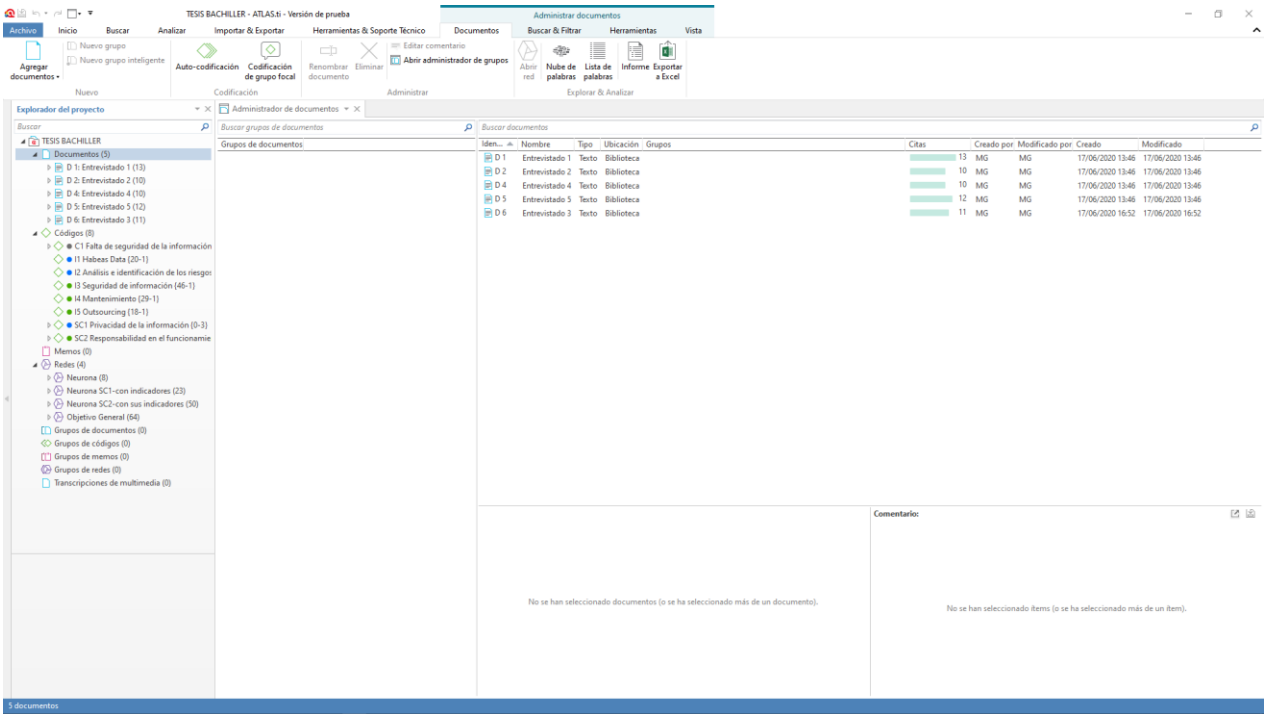


Figura 6. Documentos de entrevistas en Atlas.ti. Fuente: Elaboración propia

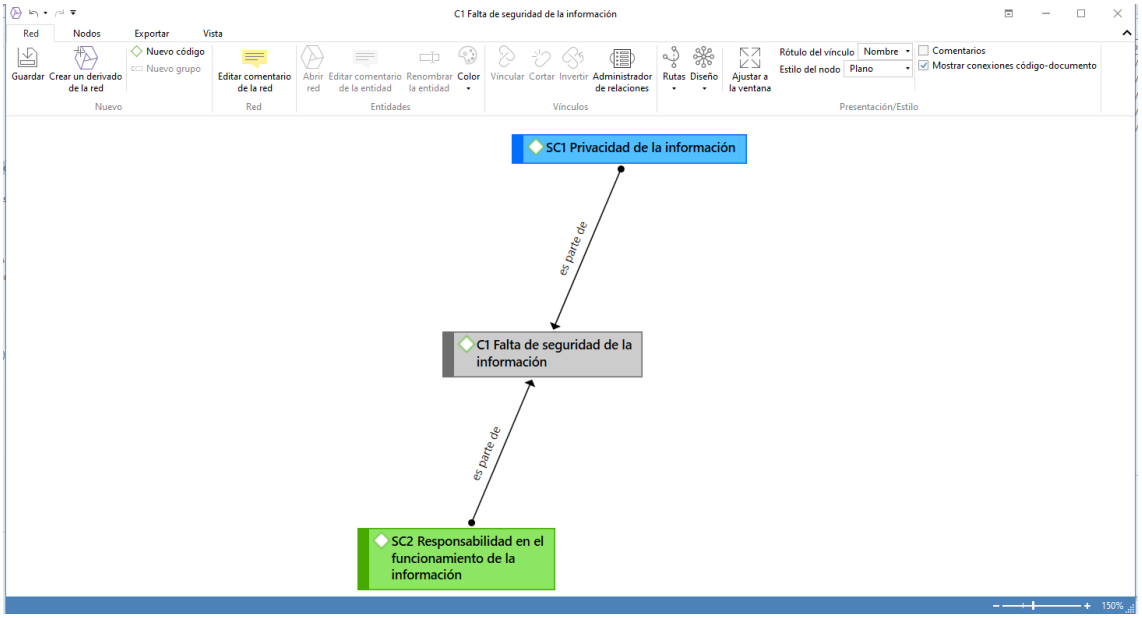


Figura 7. Falta de seguridad de la información. Fuente: Elaboración propia

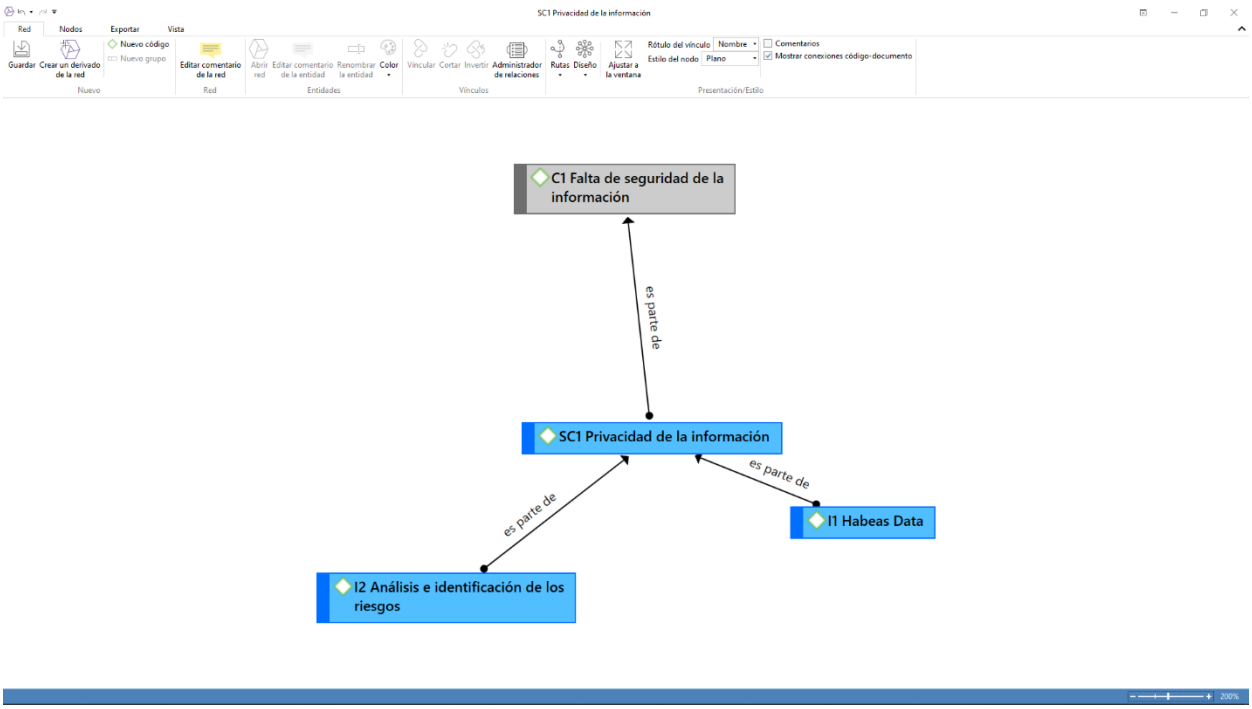


Figura 9. SC1 Privacidad de la información. Fuente: Elaboración propia

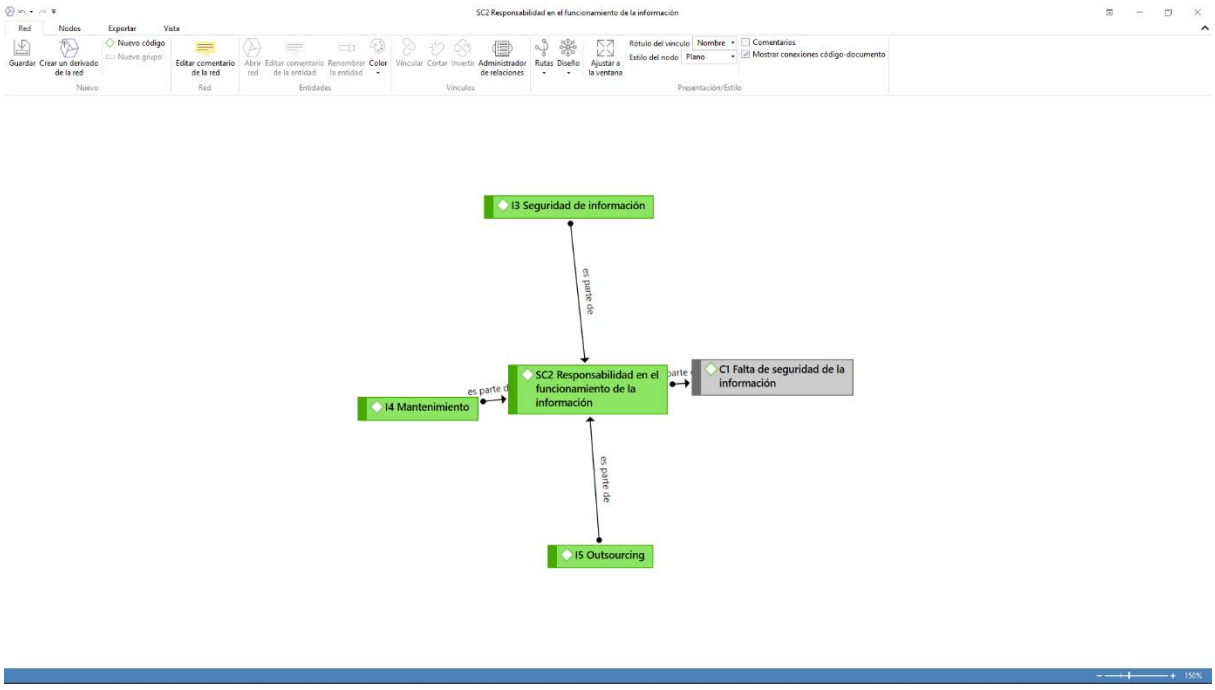


Figura 8. SC2 Responsabilidad en el funcionamiento de la información. Fuente: Elaboración propia


Explorador del proyecto
Buscar
TESIS BACHILLER
Documentos (5)
D 1: Entrevistado 1 (13)
D 2: Entrevistado 2 (10)
D 4: Entrevistado 4 (10)
D 5: Entrevistado 5 (12)
D 6: Entrevistado 3 (11)
Códigos (8)
C1 Falta de seguridad de la información {0-2}
SC1 Privacidad de la información {0-3} <es parte de>
I1 Habeas Data {20-1} <es parte de>
I2 Análisis e identificación de los riesgos {29-1} <es parte de>
SC2 Responsabilidad en el funcionamiento de la información {0-4} <es parte de>
I3 Seguridad de información {46-1} <es parte de>
I4 Mantenimiento {29-1} <es parte de>
I5 Outsourcing {18-1} <es parte de>
I1 Habeas Data {20-1}
I2 Análisis e identificación de los riesgos {29-1}
I3 Seguridad de información {46-1}
I4 Mantenimiento {29-1}
I5 Outsourcing {18-1}
SC1 Privacidad de la información {0-3}
I1 Habeas Data {20-1} <es parte de>
I2 Análisis e identificación de los riesgos {29-1} <es parte de>
SC2 Responsabilidad en el funcionamiento de la información {0-4}
I3 Seguridad de información {46-1} <es parte de>
I4 Mantenimiento {29-1} <es parte de>
I5 Outsourcing {18-1} <es parte de>
Memos (0)
Redes (4)
Neurona (8)
C1 Falta de seguridad de la información {0-2}
I1 Habeas Data {20-1}
I2 Análisis e identificación de los riesgos {29-1}
I3 Seguridad de información {46-1}
I4 Mantenimiento {29-1}
I5 Outsourcing {18-1}
SC1 Privacidad de la información {0-3}
SC2 Responsabilidad en el funcionamiento de la información {0-4}
Neurona SC1-con indicadores (23)
I1 Habeas Data {20-1}
I2 Análisis e identificación de los riesgos {29-1}
SC1 Privacidad de la información {0-3}
1:1 No se está aplicando los estándares de calidad (191:236)
1:2 Por la misma informalidad, por el poco seguimiento que se realiza (340:404)
1:3 En este punto hay dos secciones la LAN que comprende dentro de la empr... (559:1001)
1:4 Para ciertas secciones de información empleo cifrado simétrico y en ot... (1125:1289)
1:6 Otro problema por temas interno de la empresa y cultura organizacional... (1499:1570)
2:1 Está en proceso aún ya que en los últimos años no se ha tenido la impo... (187:433)
2:2 Porque en el Perú no se ha realizado una buena campaña de difusión sob... (501:589)
4:1 En un proceso que aún falta perfeccionar porque recién en los últimos... (185:319)
4:2 Porque la mayoria de la población no sabe ni está familiarizada con su... (388:497)
4:9 para disminuir el costo del producto o servicio, permitiendo ofrecer s... (1972:2125)
4:10 Las características que se debe tomar en cuenta al elegir un Outsourci... (2214:2381)
5:1 Desde hace unos años el Perú cuenta con la ley de protección de datos... (178:297)
5:2 Porque la mayoria de los peruanos viven en la ignorancia de que hay un... (365:516)
5:5 Se debe al comercio electrónico que no está bien auditado (974:1030)
5:9 no limitamos el número de empleados, Aunque deshabilitar la cuenta de... (1657:1927)
6:1 En nuestro país en comparación con el resto, existe una deficiencia en... (185:486)
6:3 Debido que el peruano no conoce su propia constitución política, por c... (696:811)
6:6 Debido a la información; todo lo que una persona natural o jurídica ha... (1311:1619)
6:11 Debido que las empresas prefieren no invertir en infraestructura para... (2365:2613)
6:12 A mi parecer lo siguiente: - Que servicio deseo tercerizar. -El presup... (2701:2924)
Neurona SC2-con sus indicadores (50)
I3 Seguridad de información {46-1}
I4 Mantenimiento {29-1}
I5 Outsourcing {18-1}
SC2 Responsabilidad en el funcionamiento de la información {0-4}
1:3 En este punto hay dos secciones la LAN que comprende dentro de la empr... (559:1001)
1:4 Para ciertas secciones de información empleo cifrado simétrico y en ot... (1125:1289)
1:5 Por el conformismo de que nunca seré atacado. Otro puede ser por el po... (1377:1496)
1:6 Otro problema por temas interno de la empresa y cultura organizacional... (1499:1570)
1:7 Yo considero lo siguiente: Se presenta una mayor motivación. Interacci... (1671:1987)
1:8 El mayor riesgo es la inversión de una nueva tecnología sin haber real... (1988:2120)
1:9 Claro que sí, es un tema delicado por el gran riesgo e impacto que pue... (2237:2505)
1:10 Actualmente el área de soporte y redes lo ejecutan, con una comunicaci... (2601:2709)
1:11 Hay caso por el tema del crecimiento de la misma empresa, otro caso es... (2761:3158)


2:3 Nadie, porque no le dan la mayor importancia. (708:753)
2:4 No, solo las contraseñas de los usuarios (843:883)
2:5 Yo creo que es por el costo de la solución para combatir ataques ciber... (971:1193)
2:6 Riesgos que sean vulnerables ante cualquier persona y sea costoso. Ven... (1294:1428)
2:7 Si se limitan los privilegios de administrador, porque solamente tiene... (1545:1651)
2:8 Los responsables de estar al pendiente de los softwares estén operativ... (1743:1845)
2:9 Se recurre al outsourcing porque los costos beneficio disminuyen áreas... (1897:1993)
2:10 Las características que se debe tomar son la seguridad, reputación, ma... (2081:2172)
4:2 Porque la mayoria de la población no sabe ni está familiarizada con su... (388:497)
4:3 Quien regula el análisis e identifican los riesgos de los ataques cibe... (616:726)
4:4 Solo se encripta las contraseñas del personal. (814:860)
4:5 Se debe a: Las vulnerabilidades en el software Mala configuració... (948:1154)
4:6 Riesgos: Exceso de información disponible. Falta de p... (1254:1608)
4:7 Si, porque hay privilegios de DBA o el Administrados de redes. (1725:1786)
4:8 Cada uno instala sus propios programas. (1881:1919)
4:10 Las características que se debe tomar en cuenta al elegir un Outsourci... (2214:2381)
5:1 Desde hace unos años el Perú cuenta con la ley de protección de datos... (178:297)
5:3 Quien se encarga en el análisis o los riesgos de las vulnerabilidades... (635:737)
5:4 Solo encriptamos las bases de datos más no de los clientes. (825:883)
5:5 Se debe al comercio electrónico que no está bien auditado (974:1030)
5:6 Como toda nueva tecnología para atreverse a ser utilizada debe garanti... (1131:1415)
5:8 Es mejor consolidarse en una tecnología debidamente probada que posici... (1416:1540)
5:9 no limitamos el número de empleados, Aunque deshabilitar la cuenta de... (1657:1927)
5:10 Aunque la cuenta de administrador puede revertir estos controles en úl... (1928:2134)
5:11 El área de TI es responsable de instalar y mantener los softwares de s... (2228:2334)
5:12 Porque son más barato de mantenerlos. (2386:2422)
5:13 Las características que se debe tomar en cuenta al elegir un Outsourci... (2511:2625)
6:1 En nuestro país en comparación con el resto, existe una deficiencia en... (185:486)
6:2 La información que debía servir para facilitar la ayuda a los más vuln... (488:627)
6:4 En el caso de mi empresa, tengo entendido que es solicitada mediante u... (930:1050)
6:5 Si se encripta, pero dicha actividad la desarrolla el área de soporte... (1138:1223)
6:6 Debido a la información; todo lo que una persona natural o jurídica ha... (1311:1619)
6:7 Ventajas: -Acceso a la información sin importar la ubicación geográfic... (1719:1984)
6:8 Si, se limita los privilegios solamente para el área encargada. (2102:2165)
6:9 El área de Soporte, es la encargada de dicho servicio. (2259:2313)
6:11 Debido que las empresas prefieren no invertir en infraestructura para... (2365:2613)
6:12 A mi parecer lo siguiente: - Que servicio deseo tercerizar. -El presup... (2701:2924)
Objetivo General (64)
C1 Falta de seguridad de la información {0-2}
I1 Habeas Data {20-1}
I2 Análisis e identificación de los riesgos {29-1}
I3 Seguridad de información {46-1}
I4 Mantenimiento {29-1}
I5 Outsourcing {18-1}
SC1 Privacidad de la información {0-3}
SC2 Responsabilidad en el funcionamiento de la información {0-4}
1:1 No se está aplicando los estándares de calidad (191:236)
1:2 Por la misma informalidad, por el poco seguimiento que se realiza (340:404)
1:3 En este punto hay dos secciones la LAN que comprende dentro de la empr... (559:1001)
1:4 Para ciertas secciones de información empleo cifrado simétrico y en ot... (1125:1289)
1:5 Por el conformismo de que nunca seré atacado. Otro puede ser por el po... (1377:1496)
1:6 Otro problema por temas interno de la empresa y cultura organizacional... (1499:1570)
1:7 Yo considero lo siguiente: Se presenta una mayor motivación. Interacci... (1671:1987)
1:8 El mayor riesgo es la inversión de una nueva tecnología sin haber real... (1988:2120)
1:9 Claro que sí, es un tema delicado por el gran riesgo e impacto que pue... (2237:2505)
1:10 Actualmente el área de soporte y redes lo ejecutan, con una comunicaci... (2601:2709)
1:11 Hay caso por el tema del crecimiento de la misma empresa, otro caso es... (2761:3158)
1:12 El outsourcing facilita esa tarea con software de control para distint... (3160:3243)
1:13 Para definir se tendría que responder a estas preguntas en función de... (3332:3824)
2:1 Está en proceso aún ya que en los últimos años no se ha tenido la impo... (187:433)
2:2 Porque en el Perú no se ha realizado una buena campaña de difusión sob... (501:589)
2:3 Nadie, porque no le dan la mayor importancia. (708:753)
2:4 No, solo las contraseñas de los usuarios (843:883)
2:5 Yo creo que es por el costo de la solución para combatir ataques ciber... (971:1193)
2:6 Riesgos que sean vulnerables ante cualquier persona y sea costoso. Ven... (1294:1428)
2:7 Si se limitan los privilegios de administrador, porque solamente tiene... (1545:1651)
2:8 Los responsables de estar al pendiente de los softwares estén operativ... (1743:1845)
2:9 Se recurre al outsourcing porque los costos beneficio disminuyen áreas... (1897:1993)
2:10 Las características que se debe tomar son la seguridad, reputación, ma... (2081:2172)
4:1 En un proceso que aún falta perfeccionar porque recién en los últimos... (185:319)
4:2 Porque la mayoria de la población no sabe ni está familiarizada con su... (388:497)
4:3 Quien regula el análisis e identifican los riesgos de los ataques cibe... (616:726)
4:4 Solo se encripta las contraseñas del personal. (814:860)
4:5 Se debe a: Las vulnerabilidades en el software Mala configuració... (948:1154)
4:6 Riesgos: Exceso de información disponible. Falta de p... (1254:1608)
4:7 Si, porque hay privilegios de DBA o el Administrados de redes. (1725:1786)

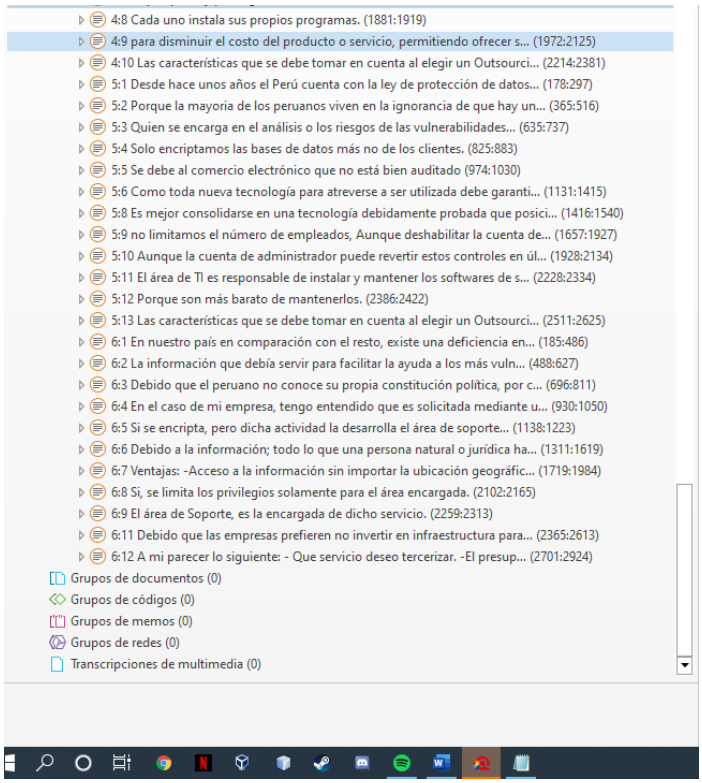


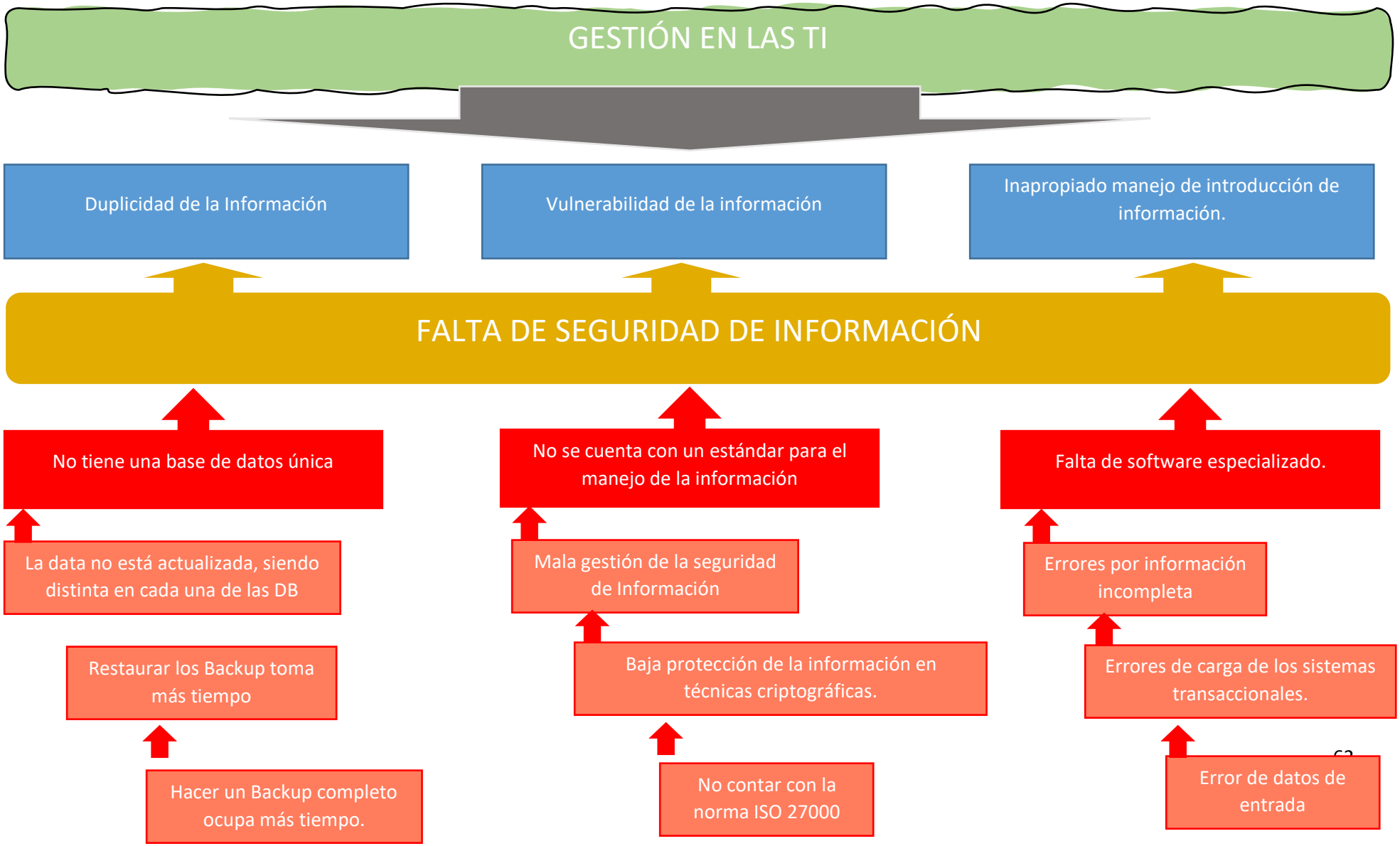
Figura 10. Triangulación con la documentación, códigos y redes con las respuestas de los entrevistados. Fuente: Elaboración propia

Anexo 5: Matrices de trabajo

1. PLANTEAMIENTO DEL PROBLEMA

<table>
<tr><td rowspan="11">Problema de investigación a nivel internacional</td><td>Informe mundial #1</td><td>Esencia del problema</td><td rowspan="11">Consolidación del problema
Internacional
Al referirnos a la seguridad informática indicamos que es más que un problema de seguridad de datos que se pueden presentar en diversos dispositivos, es por ello que la S.I. está orientada al resguardo de la propiedad intelectual, así como de la información importante de las organizaciones y personas. Al hablar de S.I. es inevitable no hacer referencias a los riesgos de información el cual consta de amenazas y vulnerabilidades que se encuentran presentes en las organizaciones, estás están íntimamente involucradas y sin ambas no existiría los riesgos, también se debe tomar en cuenta que esta puede provenir del cuerpo interna o externa de las organizaciones (Tarazona, 2007). Las Organizaciones requieren una estabilidad y un alto grado de protección el cual esté enfocada a la seguridad informática buscando prevenir las diversas amenazas dirigidas a su información. Así como existen diversas amenazas también existen diversas maneras para proteger la información; sin embargo, la principal amenaza es la desinformación que hay en las organizaciones para una correcta toma de decisiones, siendo este el motivo por el cual es necesario que las organizaciones desarrollen un modelo que permita establecer una buena práctica de la seguridad en los equipos, llevando esto a tener una correcta información, estrategias y planes para poseer una alta seguridad de información (Muñoz & Rivas, 2015). La presencia del DevOps es cada vez más importante en las empresas u organizaciones, puesto que una de sus principales funciones es reforzar la relación entre los profesionales del TI y los desarrolladores de software cuyo fin es acortar el proceso del proyecto, a su vez permite generar estrategias para el flujo de trabajo, control de versiones y entrega de producto de software, esta técnica tiene como una de sus finalidades desarrollar diversos sistemas de información en múltiples tecnologías como por ejemplo para internet, celulares y servicios de almacenamiento en la nube, entre otras (Díaz & Muñoz, 2018).</td></tr>
<tr><td>Análisis de la necesidad de construir sistemas de software reduciendo el tiempo de entrega del mercado.</td><td rowspan="3">La importancia de DevOps incrementa cada vez más, ya que se enfoca en reforzar la cooperación entre el profesional de TI y los desarrolladores de software para reducir el tiempo de entrega del proyecto, permitiendo establecer estrategias para la gestión de flujos de trabajo, control de versiones y entrega de productos de software, por lo tanto desarrolla sistemas de información en múltiples tecnologías como son para internet, dispositivos móviles y servicios en la nube, entre otras; con la finalidad de diseminar información estadística y geográfica que permitan al gobierno mexicano la toma de decisiones (Díaz & Muñoz, 2018)</td></tr>
<tr><td>Título del informe</td></tr>
<tr><td>Implementación de un enfoque DevSecOps + Risk Management en un Centro de Datos de una organización Mexicana.</td></tr>
<tr><td>Referencia</td><td colspan="2">(Díaz & Muñoz, 2018)</td></tr>
<tr><td>Informe mundial #2</td><td>Esencia del problema</td></tr>
<tr><td>Análisis de riesgos informático vulnerables.</td><td rowspan="3">Las organizaciones necesitan una estabilidad y mayor grado de protección enfocada a la seguridad informática para proteger y minimizar las amenazas a su información. Aun cuando existen diferentes maneras de proteger sus datos el principal problema es la desinformación que tienen las organizaciones para la toma de decisiones, por lo tanto, se identifica la necesidad de desarrollar un modelo que permita aplicar buenas prácticas para establecer la seguridad en equipos de seguridad informática proporcione información eficaz y eficiente sobre recomendaciones, estrategias y planes para tener un nivel de seguridad alto en su información (Muñoz & Rivas, 2015).</td></tr>
<tr><td>Título del informe
Estado actual de equipos de respuesta a incidentes de seguridad informática.</td></tr>
<tr><td>Referencia</td></tr>
<tr><td colspan="2">(Muñoz & Rivas, 2015)</td></tr>
<tr><td>Informe mundial #3</td><td>Esencia del problema</td></tr>
<tr><td>Los riesgos de la información de las organizaciones y de las personas.</td><td rowspan="3">La seguridad de la información es más que un problema de seguridad de datos en los computadores; debe estar básicamente orientada a proteger la propiedad intelectual y la información importante de las organizaciones y de las personas. Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades, las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones (Tarazona, 2007).</td></tr>
<tr><td>Título del informe
AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN.</td></tr>
<tr><td>Referencia</td></tr>
<tr><td colspan="2">(Tarazona, 2007)</td></tr>
</table>

2. Árbol de problemas a nivel local – organización



3. Matriz de causa efecto para definir el problema

Causa	Sub causa	¿Por qué?	Consolidación parcial del problema	Consolidación del problema Local
No tiene una base de datos única	1. La data no está actualizada, siendo distinta en cada una de las DB.	1. No se maneja una sola data.	En la empresa industrial no se maneja una sola data ni tampoco hay una buena metodología de análisis de datos que guardan una información repetitiva y al realizar un Backup toma más tiempo por el bajo rendimiento de las maquinas, al tener mucha información el sistema se satura.	En la empresa industrial no se maneja una sola data ni tampoco hay una buena metodología de análisis de datos ya que guardan una información repetitiva y al realizar un Backup toma más tiempo por el bajo rendimiento de las maquinas, al tener mucha información el sistema se satura. Así mismo, actualmente hay un nivel de seguridad informática baja en la empresa, ya que se trabaja con computadoras sin licencia de antivirus, al abrir correos sospechosos se corre el riesgo la información, por la baja protección no se hace copias de seguridad o se realiza mal, no se cuenta con la criptografía asimétrica ni cuentan con la norma ISO 27000 ya que es caro al implementar ni tampoco hay el personal capacitado para su implementación. Finalmente, los errores más comunes que ocurren al momento de cargar los datos como la migración de datos están vinculados a un daño en el hardware o en el tráfico de red ocasionando así campos faltantes como información incompleta en diversos archivos y que se crea una ineficiencia en la entrada de datos lo cual nos indicaría que no cuenta con un sistema ERP.
		2. No hay buena metodología de análisis de datos.		
	2. Restaurar todos los Backup toma más tiempo.	3. Al guardar una información repetitiva.		
		4. Por mal rendimiento de las maquinas.		
	3. Hacer un Backup completo ocupa más tiempo.	5. Al tener muchas informaciones.		
		6. El sistema se satura.		
No se cuenta con un estándar para el manejo de la información	4. Mala gestión de Seguridad Informática.	7. Se trabaja con computadoras sin licencia de antivirus.	Actualmente hay un nivel de seguridad informática baja en la empresa, ya que se trabaja con computadoras sin licencia de antivirus, al abrir correos sospechosos se corre el riesgo la información, por la baja protección no se hace copias de seguridad o se realiza mal, no se cuenta con la criptografía asimétrica ni cuentan con la norma ISO 27000 ya que es caro al implementar ni tampoco hay el personal capacitado para su implementación.	
		8. Abrir correos electrónicos sospechosos.		
	5. Baja protección de la informática en técnicas criptográficas.	9. No se hace copias de seguridad, o hacerlas mal.		
		10. No se cuenta con la criptografía asimétrica.		
	6. No contar con la norma ISO 27000	11. Es caro de implementarlo.		
		12. No hay personal capacitado para su implementación.		
Falta de software especializado.	7. Errores por información incompleta	13. Se encuentran registros o campos faltantes.	Los errores comunes se encuentran al registrar el campos faltante, hardware dañado, ya que existe algún problema físico en el hardware que se ocupa de este tráfico de red y es muy posible que se sufra una información incompleta, hay variedad de errores que ocurren al cargar los datos como la migración de datos, en la empresa no se cuenta con el sistema ERP y hay ineficiencia en la entrada de red y se crea el cuello de botella tanto como hay errores tipográficos.	
		14. Hardware dañado		
	8. Errores de carga de los sistemas transaccionales.	15. Hay variedad de errores que ocurren al cargar los datos.		
		16. No se cuenta con un ERP.		
	9. Error de datos de entrada	17. Hay ineficiencia en la entrada de datos.		
		18. Hay errores tipográficos.		

4. Problema, objetivo.

Análisis de la seguridad informática de una mediana empresa, Lima 2019-2020

Problema general	**Objetivo general**
¿Cuál es la situación de la seguridad informática de una mediana empresa, Lima 2019-2020?	Analizar la seguridad informática de una mediana empresa, Lima 2019-2020
Problemas específicos	**Objetivos específicos**
¿Cuál es la situación de la privacidad de la información de una mediana empresa, Lima 2019-2020?	Analizar la privacidad de la información de una mediana empresa, Lima 2019-2020
¿Cuál es la situación de la responsabilidad en el funcionamiento de la información de una mediana empresa, Lima 2019-2020?	Analizar la responsabilidad en el funcionamiento de la información de una mediana empresa, Lima 2019-2020

5. Justificación

<table>
<tr><th colspan="3">Justificación teórica</th></tr>
<tr><th colspan="2">¿Qué teorías sustentan la investigación?</th><th>¿Cómo estas teorías aportan a su investigación?</th></tr>
<tr><td colspan="2">1. Teoría de Información
2. Teoría de Sistemas
3. Teoría de Decisión</td><td>1. Permitió comprender la importancia del procesamiento de la información, ya que esto nos da acceso a ver la capacidad de los sistemas de comunicación y de poder transmitir o procesar la información.
2. Permitió entender que la teoría de sistemas es el análisis en sistemas que se debe tener una mentalidad sistémica, porque al tener una mente sistémica podemos ver, analizar, actuar, entender el problema real.
3. Permitió conocer el valor significativo de la toma de decisiones para cualquier tipo de desafío, porque al tomar una decisión hay diversos factores y así tomar el mejor resultado posible siendo así un resultado positivo.</td></tr>
<tr><td>Redacción final</td><td colspan="2">El estudio tiene justificación teórica porque se sustenta que en la teoría de información nos permite comprender la importancia del procesamiento de la información, ya que esto nos da acceso a ver la capacidad de los sistemas de comunicación y de poder transmitir o procesar la información; asimismo en la teoría de sistemas permite entender que la teoría de sistemas es el análisis en sistemas que se debe tener una mentalidad sistémica, porque al tener una mente sistémica podemos ver, analizar, actuar, entender el problema real; de igual modo la teoría de decisión permite conocer el valor significativo de la toma de decisiones para cualquier tipo de desafío, porque al tomar una decisión hay diversos factores y así tomar el mejor resultado posible siendo así un resultado positivo.</td></tr>
</table>

Justificación práctica	
¿Por qué realizar el trabajo de investigación?	**¿Cómo el estudio aporta a la organización?**
1. Para identificar las deficiencias en base a la seguridad informática en descoordinación entre las áreas. 2. Para identificar las vulnerabilidades de un posible ataque cibernético. 3. Para determinar un mejor control de la información.	1. Para determinar en donde se encuentra la duplicidad de datos de información. 2. Para identificar cuáles son las malas configuraciones del sistema para utilizar un exploit específico. 3. Para identificar el cuello de botella del tráfico de datos.
Redacción final	El estudio tiene justificación práctica porque permite identificar las deficiencias en base a la seguridad informática en descoordinación entre las áreas, para determinar en donde se encuentra la duplicidad de datos de información; asimismo se identifica las vulnerabilidades de un posible ataque cibernético, nos permite identificar cuáles son las malas configuraciones del sistema para utilizar un exploit especifico; del mismo modo permite determinar un mejor control de la información, para identificar el cuello de botella del tráfico de datos.

Justificación metodológica	
¿Por qué realizar la investigación bajo el enfoque cualitativo?	**¿Cómo las técnicas e instrumentos permitieron recopilar los datos?**
1. Porque el estudio se basa en un caso particular, como lo es en la empresa de estudio. 2. Porque los datos surgen poco a poco. 3. Porque permite obtener las perspectivas de las personas involucradas directamente con la investigación. 4. Porque el problema se analiza dividido en partes.	5. El análisis documental que consta en examinar los datos ya existentes. 6. La técnica Delphi busca obtener información esencial para la toma de decisiones. 7. Las entrevistas es una de las técnicas que busca la apreciación de la opinión respecto al problema. 8. Los cuestionarios es una de las técnicas que busca obtener datos precisos.
Redacción final	El estudio se justifica metodológicamente porque se realizó bajo el enfoque cualitativo, el estudio se basa en un caso particular, como lo es en la empresa de estudio, también se basa en los datos que surgen poco a poco, asimismo permite obtener las perspectivas de las personas involucradas directamente con la investigación y el problema se analiza dividido en partes. En ese sentido, las técnicas e instrumentos usadas fueron: el análisis documental, que consta en examinar los datos ya existentes, la técnica Delphi busca obtener información esencial para la toma de decisiones, las entrevistas es una de las técnicas que busca la apreciación de la opinión respecto al problema y los cuestionarios es una de las técnicas que busca obtener datos precisos.

6. Matriz de teorías

Teoría 1: De la Información					
Autor de la teoría	**Año**	**Cita**	**Parafraseo (1)**	**Aplicación en su tesis (2)**	**Redacción final**
Shannon, C. Elwood, Warren Weaver	1948	Deseamos considerar ciertos problemas relacionados con el sistema de comunicación. Para hacer esto, primero es necesario representar los diversos elementos involucrados como entidades matemáticas, adecuadamente idealizados de su físico contrapartes. Podemos clasificar aproximadamente los sistemas de comunicación en tres principales categorías: discreta, continua y mixta. Por un sistema discreto significará uno en el que tanto el mensaje como la señal son una secuencia de símbolos discretos. Un caso típico es la telegrafía donde el mensaje es una secuencia de letras y la señal una secuencia de puntos, guiones y espacios. Un sistema continuo es aquel en el que el mensaje y la señal son tratados como funciones continuas, por ejemplo, radio o televisión. Un sistema mixto es aquel en el que aparecen variables discretas y continuas, por ejemplo, transmisión de voz PCM. (Shannon, Warren, 1948, pp. 7-8)	Se requiere reflexionar ciertos problemas interrelacionados con el sistema de comunicación. Para que se pueda realizar, en primer lugar, es esencial mostrar los diversos elementos involucrados como entidades matemáticas y se clasifica en 3 categorías "discreta, continua y mixta". Por el método discreto significa que gracias a la secuencia de símbolos se logra crear mensajes y señales, de esta manera se obtiene la telegrafía, el cual está compuesto por un grupo de letras con el cual se crean palabras, a su vez se hacen él hace el uso de puntos, guiones y espacios llevando todo ello transmitir un mensaje claro y comprensible, siendo este conocido como el método continuo, además de este método existe el método mixto el cual está constituido por variables discretas y continuas (Shannon & Warren, 1948)**.**	La teoría de la información que es conocida como la matemática de la comunicación, es la rama de las teorías de la matemática y de la ciencia de la computación, aplicando así, esta última estudia la información todo lo relacionado, aplicando así un como canal de información, comprensión de datos y criptografía	En la teoría de la información es considerada parte de la teoría de la probabilidad con amplios potenciales para los sistemas de comunicación, esta teoría al igual que otras también cuenta con un origen físico que fue elaborado por científicos de la comunicación, estos buscaban estudiar la estructura estadística de los equipos de comunicación eléctrica, sin embargo esta fue empleada de manera anticipada en zonas marginales, es por ello que las últimas investigaciones realizadas hace 5 o 6 años demuestran que es necesario realizar investigaciones profundas sobre los fundamentos de esta disciplina. Asimismo, se requiere reflexionar ciertos problemas interrelacionados con el sistema de comunicación. Para que se pueda realizar, en primer lugar, es esencial mostrar los diversos elementos involucrados como entidades matemáticas y se clasifica en 3 categorías "discreta, continua y mixta". Por el método discreto que gracias a la secuencia de símbolos se logra crear mensajes y señales, de esta manera se obtiene la telegrafía, el cual está compuesto por un grupo de letras con el cual se crean palabras, a su vez se hacen él hace el uso de puntos, guiones y espacios llevando todo ello transmitir un mensaje claro y comprensible, siendo este conocido como el método continuo, además de este método existe el método mixto el cual está constituido por variables discretas y continuas (Shannon, Warren, 1948; Fazlollah, 1994).
Referencia:	(Shannon & Warren, 1948)				La teoría de la información es conocida como la matemática de la comunicación, es una rama de
Autor/es	**Año**	**Cita**	**Parafraseo (3)**	**Aplicación en su tesis (4)**	

Fazlollah M. Reza	1994	La teoría de la información es una nueva rama de la teoría de la probabilidad con extensas aplicaciones potenciales para los sistemas de comunicación. Al igual que varias otras ramas de las matemáticas, la teoría de la información tiene un origen físico. Fue iniciado por científicos de la comunicación que estudiaban la estructura estadística de los equipos de comunicación eléctrica. La aplicación inmediata de esta nueva disciplina a las zonas marginales fue bastante prematura. De hecho, la investigación en los últimos 5 o 6 años ha indicado la necesidad de investigaciones más profundas sobre los fundamentos de la disciplina misma. (Fazlollah, 1994, p1)	En la teoría de la información es considerada parte de la teoría de la probabilidad con amplios potenciales para los sistemas de comunicación, esta teoría al igual que otras también cuenta con un origen físico que fue elaborado por científicos de la comunicación, estos buscaban estudiar la estructura estadística de los equipos de comunicación eléctrica, sin embargo esta fue empleada de manera anticipada en zonas marginales, es por ello que las últimas investigaciones realizadas hace 5 o 6 años demuestran que es necesario realizar investigaciones profundas sobre los fundamentos de esta disciplina (Fazlollah, Reza;, 1994).	El personal tiene la capacitación adecuada para emplear las estructuras de redes de telecomunicación.	las teorías de la matemática y de la ciencia de la computación, aplicando así, esta última estudia la información relacionada a la medición y capacitación de los sistemas de comunicación para así transmitir y procesar dicha información, aplicando así un como canal de información, comprensión de datos y criptografía. En este sentido desde la perspectiva de la teoría de la información es importante y necesaria que el personal tenga capacitación adecuada para emplear las estructuras de redes de telecomunicación.
Referencia:	(Fazlollah, Reza;, 1994)				

Teoría 2: de Sistemas					
Autor de la teoría	**Año**	**Cita**	**Parafraseo (1)**	**Aplicación en su tesis (2)**	**Redacción final (1+2+3+4)**
Ludwig V. Bertalanffy	1976	La teoría general de los sistemas es una ciencia general de la "totalidad". La idea de sistema conserva su valor incluso donde no puede ser formulada matemáticamente, o no deja de ser una "idea guía" en vez de ser construcción matemática. La teoría general de los sistemas no persigue analogías vagas y superficiales. Poco valen, ya que junto a las similitudes entre fenómenos siempre se hallan también diferencias. El isomorfismo que discutimos es más que mera analogía. Es consecuencia del hecho de que, en ciertos aspectos, puedan aplicarse abstracciones y modelos conceptuales coincidentes a fenómenos diferentes. Sólo se aplicarán las leyes de sistemas con mira a tales aspectos. (Bertalanffy, 1976, pp. 23-24, 35-37)	La TGS es considerada como una ciencia de la totalidad, además el sistema mantiene su importancia incluso en donde no pueda ser formulada matemáticamente, es decir, esta no deja de ser un modelo en lugar de ser una construcción matemática, así mismo se puede decir que la TGS no busca analogías vagas y superficiales ya que estas tienen poco valor debido a la diferencia con otros fenómenos. El isomorfismo es el resultado de las aplicaciones de abstracciones y modelos conceptuales que coincide con diferentes fenómenos.	La TGS genera herramientas para la aplicación en cualquier tipo de sistemas y en cualquier tipo de organización, es posible identificar los elementos de la TGS en cualquier tipo de empresa así ayudando a los administradores a entender el fundamento de su negocio.	La teoría general de Sistemas (TGS) es considerada como una ciencia de la totalidad porque cuyas propiedades aplicables a una simple adición de las partes o componentes, además el sistema mantiene su importancia incluso en donde no pueda ser formulada matemáticamente, es decir, esta no deja de ser un modelo en lugar de ser una construcción matemática, así mismo se puede decir que la TGS no busca analogías vagas y superficiales ya que estas tienen poco valor debido a la diferencia con otros fenómenos. El isomorfismo es el resultado de la abstracción y modelos conceptuales que coincide con diferentes fenómenos. Para hablar de un sistema es necesario cumplir los siguientes requisitos: Funcional y No Funcional, si estas
Referencia:	(Von Bertalanffy, 1976)				

Autor/es	Año	Cita	Parafraseo (3)	Aplicación en su tesis (4)	características no se cumplen pondrían en duda el carácter de objeto del sistema, así mismo se menciona que también se pueda hacer referencia a un sistema a un conjunto de características. Por lo tanto, al indicar que existe un sistema hablamos que el objeto de investigación posee de ciertas características que valoran el concepto de sistema. Así mismo la definición de sistema busca abstraer y comparar diversos hechos que sean diferentes (Bertalanffy, 1976; Luhmann, 1996). La teoría general de sistemas genera herramientas para la aplicación en cualquier tipo de sistemas y en cualquier tipo de organización, es posible identificar los elementos de la TGS en cualquier tipo de empresa así ayudando a los administradores a entender el fundamento de su negocio. Nos permite llevar un análisis y desarrollo del sistema con el objetivo de buscar la solución que sea las mismas características del sistema y así se podrá lograr los objetivos de la organización.
Niklas Luhmann	1996	En general, se puede hablar de sistema cuando se tiene ante los ojos características que, si se suprimieran, pondrían en cuestión el carácter de objeto de dicho sistema. A veces, también se llama sistema al conjunto de dichas características. En el mismo sentido entonces: La afirmación "hay sistemas" sólo quiere decir que hay objetos de investigación con tales características que justifican el empleo del concepto de sistema. Así como al contrario: el concepto de sistema nos sirve para abstraer hechos que son comparables entre sí, o hechos de carácter distinto bajo el aspecto igual/desigual. (Luhmann, 1996, pp27-28)	Para hablar de Sistema es necesario hacer referencia a ciertas características, si estas características no se cumplen pondrían en duda el carácter de objeto del sistema, así mismo se menciona que también se pueda hacer referencia a un sistema a un conjunto de características. Por lo tanto, al indicar que existe un sistema hablamos que el objeto de investigación posee de ciertas características que valoran el concepto de sistema. Así mismo la definición de sistema busca abstraer y comparar diversos hechos que sean diferentes.	Nos permite llevar un análisis y desarrollo del sistema con el objetivo de buscar la solución que sea las mismas características del sistema y así se podrá lograr los objetivos de la organización.	
Referencia:	(Luhmann, 1996)				

Teoría 3: De Decisión					
Autor de la teoría	**Año**	**Cita**	**Parafraseo (1)**	**Aplicación en su tesis (2)**	**Redacción final (1+2+3+4)**
Herbert A. Simon	1997	Existen por lo menos tres razones para la especialización vertical en la organización. En primer lugar, si existe una especialización horizontal, la especialización vertical es absolutamente necesaria para realizar la coordinación entre los empleados operativos. En segundo lugar,	Para que en una organización existan una especialización horizontal, es necesaria la especialización vertical, ya que ambas permitirán llevar una coordinación eficaz entre los empleados, además la especialización horizontal permite a los empleados desarrollar mayores habilidades y destrezas para así	Esta teoría ayudó ver que el personal representa una pieza importante al ejecutar el proceso de decisión al realizar sus labores y que los decisores tengan habilidades estratégicas para una	La finalidad de la teoría de la decisión es crear todas las posibles hipótesis sobre la toma de decisiones racional, las teorías descriptivas tienen como finalidad explicar y predecir el cómo es que la gente toma las decisiones, esta es una disciplina

		de la misma manera que la especialización horizontal permite que el grupo operativo desarrolle mayor habilidad y destreza en la ejecución de sus tareas, la especialización vertical da lugar a una mayor destreza en la toma de decisiones. En tercer Jugar, la especialización vertical permite que el personal operativo sea responsable de sus decisiones: ante el Consejo de administración, cuando se trata de una organización de negocios; ante el cuerpo legislativo, cuando se trata de un organismo público. (Herbert, 1997, pp. 9-12)	realizar sus labores, por otro lado la especialización vertical da pie a generar una mejor destrezas para una correcta toma de decisiones, generando en el personal una responsabilidad sobre sus decisiones ante un consejo administrativo, un cuerpo legislativo o cualquier otro.	mejor destreza en la toma de decisión.	empírica por lo tanto es basada en la experiencia y realidad, es por ello que proviene de la psicología experimental. El objetivo de las teorías normativas es producir prescripciones sobre la responsabilidad de la toma de decisiones, la teoría de decisiones descriptivas y normativas tienen diversas diferencias generando estas que se estudien independiente cada una. Por lo tanto para que en una organización existan una especialización horizontal, es necesaria la especialización vertical, ya que ambas permitirán llevar una coordinación eficaz entre los empleados, además la especialización horizontal permite a los empleados desarrollar mayores habilidades y destrezas para así realizar sus labores, por otro lado la especialización vertical da pie a generar una mejor destrezas para una correcta toma de decisiones, generando en el personal una responsabilidad sobre sus decisiones ante un consejo administrativo, un cuerpo legislativo o cualquier otro (Herbert, 1997; Peterson, 2009). Esta teoría ayudó ver que el personal representa una pieza importante al ejecutar el proceso de decisión al realizar sus labores y que los decisores tengan habilidades estratégicas para una mejor destreza en la toma de decisión. Al mismo tiempo, Con la teoría de decisiones podremos analizar y hacer frente a cada problema que la empresa obtenga ya que
Referencia:	(Herbert, 1997)				
Autor/es	**Año**	**Cita**	**Parafraseo (3)**	**Aplicación en su tesis (4)**	
Martin Peterson	2009	El objetivo final de la teoría de la decisión es formular hipótesis sobre una toma de decisiones racional que sea tan posible, las teorías descriptivas de decisión buscan explicar y predecir cómo la gente realmente toma decisiones. Esta es una disciplina empírica, derivada de psicología experimental. Las teorías normativas buscan producir prescripciones acerca de lo que los responsables de la toma de decisiones están obligados, o deberían, hacer. La teoría de decisión descriptiva y normativa es, por lo tanto, dos campos separados de consulta, que puede estudiarse independientemente uno del otro. (Peterson, 2009, pp. 2-3)	La finalidad de la teoría de la decisión es crear todas las posibles hipótesis sobre la toma de decisiones racional, las teorías descriptivas tienen como finalidad explicar y predecir el cómo es que la gente toma las decisiones, esta es una disciplina empírica por lo tanto es basada en la experiencia y realidad, es por ello que proviene de la psicología experimental. El objetivo de las teorías normativas es producir prescripciones sobre la responsabilidad de la toma de decisiones, la teoría de decisiones descriptivas y normativas tienen diversas diferencias generando estas que se estudien independiente cada una.	Con la teoría de decisiones podremos analizar y hacer frente a cada problema que la empresa obtenga ya que el personal tendrá la capacidad y experiencia que se requiere.	

Referencia:	(Peterson, 2009)	el personal tendrá la capacidad y experiencia que se requiere.

7. Matriz de antecedentes (5 internacional – 5 nacional)

Datos del antecedente 01: Internacionales			
Título	ALIGNING INFORMATION SECURITY WITH THE IMAGE OF THE ORGANIZATION AND PRIORITIZATION BASED ON FUZZY LOGIC FOR THE INDUSTRIAL AUTOMATION SECTOR	Metodología	
Autor	Knorst André Marcelo, Vanti Adolfo Alberto, Espín Andrade Rafael Alejandro, Silvio Luiz Johann	Tipo	
Año	2011	Enfoque	
Objetivo	Modelo de integración y creación de un instrumento de búsqueda para evaluar la información de seguridad	Diseño	
Resultados	Como resultado, es posible establecer una relación utilizando estratégicamente los criterios de seguridad e integrarlos a través del modelo BSC, COBIT e ISO27002 ya que estos facilitan el mapeo de objeticos genéricos para el negocio de TI desde la perspectiva del BSC con los objetivos generales de TI.	Método	
		Población	
		Muestra	
		Unidades informantes	
		Técnicas	
		Instrumentos	
Conclusiones	En conclusión, el gobierno de TI permite la expansión del cumplimiento y el gobierno corporativo mediante el uso de diferentes modelos, como la auditoria de procesos e seguridad de información de TI y esto proporciona sistemas más robustos con control interno con la finalidad de alcanzar un nivel técnico y operativo, incluye el mapeo de proceso COBIT con las prácticas de ISO27002.	Método de análisis de datos	
Redacción final al estilo artículo	Knorst, Vanti, Espín Andrade, Silvio (2011), evidenciaron que es posible establecer una relación utilizando estratégicamente los criterios de seguridad e integrarlos a través del modelo BSC, COBIT e ISO27002 ya que estos facilitan el mapeo de objeticos genéricos para el negocio de TI desde la perspectiva del BSC con los objetivos generales de TI.		

<table>
<tr><td colspan="4">Datos del antecedente 02: Internacionales</td></tr>
<tr><td>Título</td><td>DETERMINING FACTORS OF BANK EMPLOYEE READING HABITS OF INFORMATION SECURITY POLICIES</td><td>Metodología</td><td></td></tr>
<tr><td>Autor</td><td>William Allassani</td><td>Tipo</td><td></td></tr>
<tr><td>Año</td><td>2014</td><td>Enfoque</td><td></td></tr>
<tr><td>Objetivo</td><td>Con la llegada de la World Wide Web, el e-commerce y e-banking y sus riesgos de seguridad informático, como el delito cibernético, la necesidad de proteger los bancos red y datos se vuelven más relevantes. Además de brindar soluciones técnicas tales como software antivirus, sistemas de firewall, sistema de detección de intrusos, criptología, las organizaciones también intentan influir y gestionar el comportamiento y las actividades de sus empleados a través de políticas de seguridad de la información que detallan las tareas y no hacer uso de los sistemas informáticos.</td><td>Diseño</td><td>No experimental</td></tr>
<tr><td rowspan="6">Resultados</td><td rowspan="6">Como resultado, la mayoria del personal no tiene buenos hábitos de lectura sobre las políticas de seguridad de la empresa, Los empleados que han trabajado menos de 5 años tienen menos probabilidades de leer, incluso si son personas mayores, los ejecutivos están involucrados en el proceso de monitoreo.</td><td>Método</td><td></td></tr>
<tr><td>Población</td><td></td></tr>
<tr><td>Muestra</td><td></td></tr>
<tr><td>Unidades informantes</td><td></td></tr>
<tr><td>Técnicas</td><td>Encuesta</td></tr>
<tr><td>Instrumentos</td><td>Guía de encuesta</td></tr>
<tr><td>Conclusiones</td><td>En conclusión, en base que los empleados al no tener buenos hábitos de lectura, se desea recomendar que a los empleados sean evaluados anualmente y ser recompensados.</td><td>Método de análisis de datos</td><td></td></tr>
<tr><td>Redacción final al estilo artículo</td><td colspan="3">Allassani (2014), constata que la mayoria del personal no tiene buenos hábitos de lectura sobre las políticas de seguridad de la empresa, Los empleados que han trabajado menos de 5 años tienen menos probabilidades de leer, incluso si son personas mayores, los ejecutivos están involucrados en el proceso de monitoreo, en base que los empleados al no tener buenos hábitos de lectura, se desea recomendar que a los empleados sean evaluados anualmente y ser recompensados.</td></tr>
</table>

Datos del antecedente 03: Internacionales			
Título	SEGURANÇA DA INFORMAÇÃO DE PRODUÇÃO E OPERAÇÕES: UM ESTUDO SOBRE TRILHAS DE AUDITORIA EM SISTEMAS DE BANCO DE DADOS.	Metodología	
Autor	Roratto Rodrigo, Dotto Dias Evandro	Tipo	
Año	2014	Enfoque	
Objetivo	El objetivo es que el sistema debe estar preparado para resistir los ataques creando registros y versiones falsas que pasan por el proceso de auditoría. Esta clase de ataque incluye la creación de versiones falsas del archivo de datos que coinciden con los metadatos publicados, pero difieren de los datos utilizados en su creación, también incluye crear historias falsas, insertar o eliminar versiones en una secuencia sin detección. En esta investigación se describió la importancia de la auditoría como una actividad que tiene como objetivo garantizar la seguridad y la continuidad del negocio.	Diseño	No experimental
Resultados	Como resultado, hay estudios en el área con algunas implementaciones, pero ninguno de ellos se presentó como una solución óptima al problema de seguridad de información, También se presentaron dos sistemas comerciales de Oracle e IBM que prometen resolver problemas, como el acceso inadecuado a información confidencial e integridad de los registros de auditoría.	Método	
		Población	
		Muestra	
		Unidades informantes	
		Técnicas	Encuesta
		Instrumentos	Guía de encuesta
Conclusiones	En conclusión, se presenta la importancia de garantizar la seguridad, inviolabilidad e integridad de la información contenida en un sistema de gestión informatizado, se concluye que, con la creciente dependencia de los sistemas críticos de almacenamiento de datos, y desarrollar nuevas soluciones para el monitoreo y protección de estos datos, está claro que esta es un área de estudio muy prometedora e importante, y se recomienda Realizar nuevas investigaciones en el área de control y seguridad de la información a través del uso de las tecnologías de Business Intelligence.	Método de análisis de datos	
Redacción final al estilo artículo	Roratto & Dotto Dias (2014), evidenciaron que se presenta la importancia de garantizar la seguridad, inviolabilidad e integridad de la información contenida en un sistema de gestión informatizado, se concluye que, con la creciente dependencia de los sistemas críticos de almacenamiento de datos, desarrollar nuevas soluciones para el monitoreo y protección de estos datos y desarrollar nuevas soluciones para el monitoreo y protección de estos datos, está claro que esta es un área de estudio muy prometedora e importante, y se recomienda Realizar nuevas investigaciones en el área de control y seguridad de la información a través del uso de las tecnologías de BI.		

Datos del antecedente 04: Internacionales			
Título	Application of business intelligence For analyzing vulnerabilities to increase the security level in an academic CSIRT	Metodología	Investigación-Acción Ralph Kimball Scrum
Autor	Reyes Mena Francisco, Fuertes Díaz Walter, Guzmán Jaramillo Carlos.	Tipo	
Año	2017	Enfoque	Cualitativo
Objetivo	Como objetivo se diseñó una solución potencial a través de Business Intelligence para adquirir datos e información de una amplia variedad de fuentes y utilizarlas en la toma de decisiones del análisis de vulnerabilidad de un CSIRT académico (Equipo de respuesta a incidentes de seguridad informática).	Diseño	Experimental
Resultados	Como resultado, muestran que dicha aplicación ha logrado ayudar a los responsables del CSIRT a establecer prioridades inmediatas y asignar recursos a áreas clave, que pueden ser víctimas potenciales de ataques digitales. Las técnicas de Big Data proporcionan escalabilidad en escenarios de alto volumen de datos en el CSIRT, por lo tanto, sugerimos aplicarlas en futuros estudios.	Método	
		Población	
		Muestra	
		Unidades informantes	
		Técnicas	-Se realizó un análisis de intrusos: Scanner de vulnerabilidad pasiva y Snort. -Se aplicó desarrolló de varias rutinas que especificaron la aplicación del proceso "Extraer, Transformar y Cargar" - Se construyó una aplicación de software
		Instrumentos	Scanner de vulnerabilidad pasiva y Snort, MySQL
Conclusiones	En conclusión, se diseñó una solución implementada a través de Business Intelligence que actúa como un factor estratégico en el análisis de vulnerabilidad de un CSIRT y esto fue esto fue posible aplicando la metodología de Investigación-Acción y las fases de Ralph Kimball.	Método de análisis de datos	
Redacción final al estilo artículo	Reyes Mena, Fuertes Díaz, Guzmán Jaramillo (2017), se diseñó una solución implementada a través de Business Intelligence que actúa como un factor estratégico en el análisis de vulnerabilidad de un CSIRT y esto fue posible aplicando la metodología de Investigación-Acción y las fases de Ralph Kimball.		

Datos del antecedente 05: Internacionales			
Título	PAPEL MODERADOR DA ORIENTAÇÃO EMPREENDEDORA SOBRE UN RELAÇÃO ENTRE A AVALIAÇÃO DO RISCO DA SEGURANÇA DA INFORMAÇÃO EO DESEMPENHO DA EMPRESA NO QUÊNIA	Metodología	Métodos mixtos
Autor	Stanley Ndungu, Kenneth Wanjau, Robert Gichira, Waweru Mwangi.	Tipo	Descriptivo
Año	2017	Enfoque	Cuantitativas y cualitativas
Objetivo	El objetivo es investigar el efecto de la orientación empresarial en la relación entre la evaluación de riesgos de seguridad de la información y el desempeño de la empresa en Kenia.	Diseño	
Resultados	Como resultado, a través del análisis y la evaluación del riesgo organizacional, las amenazas y vulnerabilidades relacionadas con la seguridad de la información podrían estimarse y evaluarse, y los resultados de la evaluación podrían usarse para planificar los requisitos de seguridad de la información y las medidas de control de riesgos, con el objetivo final Reducir o minimizar el riesgo de seguridad de la información a un nivel aceptable en una organización.	Método	
		Población	94 PYMES
		Muestra	
		Unidades informantes	
		Técnicas	
		Instrumentos	SPSS, Ms-Excel, AMOS, SmartPLS, STATA, R-GUI y ATLAS.t
Conclusiones	En conclusión, el estudio sobre la Teoría integrada del sistema de gestión de la seguridad de la información, identificaron la evaluación de riesgos de seguridad de la información como uno de los factores de éxito de la gestión de la seguridad de la información.	Método de análisis de datos	
Redacción final al estilo artículo	Stanley Ndungu, Kenneth Wanjau, Robert Gichira, Waweru Mwangi. (2017). Evidenciaron que el estudio sobre la Teoría integrada del sistema de gestión de la seguridad de la información, identificaron la evaluación de riesgos de seguridad de la información como uno de los factores de éxito de la gestión de la seguridad de la información.		

Datos del antecedente 01: Nacionales			
Título	MEJORA DE SEGURIDAD DE INFORMACIÓN EN LA COMANDANCIA DE OPERACIONES GUARDACOSTAS BASADA EN LA NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008	Metodología	Planear, Hacer, Verificar y Actuar usado por las normas NTP-ISO/IEC 27001:2008
Autor	FERNÁNDEZ PEÑALOZA, DAVID PACHECO VARGAS, OSCAR	Tipo	
Año	2014	Enfoque	
Objetivo	DISEÑAR UN PLAN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA COMANDANCIA DE OPERACIONES GUARDACOSTAS -COMOPERGUARD- BASADA EN LA NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008.	Diseño	
Resultados	Como resultado es minimizar los riesgos, amenazas y vulnerabilidades de los activos de información como también el compromiso del personal de la Comandancia con respecto a la seguridad de información.	Método	
		Población	
		Muestra	
		Unidades informantes	
		Técnicas	Censo - inventario
		Instrumentos	
Conclusiones	La conclusión es que el modelo aplicado, ha permitido desarrollar el Plan de Sistema de Gestión de Seguridad de la información de la Comandancia basado en la norma NTP-ISO/IEC 27001:2008.	Método de análisis de datos	
Redacción final al estilo artículo	FERNÁNDEZ PEÑALOZA, PACHECO VARGAS (2014), acreditan que el resultado es minimizar los riesgos, amenazas y vulnerabilidades de los activos de información como también el compromiso del personal de la Comandancia con respecto a la seguridad de información.		

Datos del antecedente 02: Nacionales			
Título	DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN DE LA CLÍNICA MEDCAM PERÚ SAC	Metodología	Deming o PDCA (Plan-Do-Check-Act)
Autor	CRUZ DIAZ MIGUEL ANGEL, FUKUSAKI INFANTAS SENYI	Tipo	
Año	2017	Enfoque	
Objetivo	Diseñar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI) con el fin de proteger los activos de información que influyan directamente en el cumplimiento de los objetivos de la empresa.	Diseño	
Resultados	Como resultado, un Sistema de Gestión de Seguridad de la Información puede ser aplicado a cualquier empresa sin importar el tamaño ni el rubro al que se dedique, así mismo identificaron los activos de información y su valorización, mapeo de riesgos, declaración de aplicabilidad y la implementación de controles, lo que logró la reducción de los riesgos identificados.	Método	Plan-Do-Check-Act
		Población	Personal de la Clínica MEDCAM PERU SAC
		Muestra	
		Unidades informantes	
		Técnicas	Encuesta
		Instrumentos	Guía de encuestas
Conclusiones	En conclusión, se logra la mitigación de los riesgos a los que estaban expuestos los activos de información de la clínica, a través de la identificación, diseño e implementación de controles para los riesgos más críticos.	Método de análisis de datos	
Redacción final al estilo artículo	CRUZ DIAZ, FUKUSAKI INFANTAS (2017) demostraron que un Sistema de Gestión de Seguridad de la Información puede ser implementada a diversas empresas sin tomar importancia al tamaño o rubro en el que se desempeñe, asimismo identificaron distintos métodos para reducir los riesgos que se presenten en las organizaciones, entre estos existen los mapeos de riesgos, declaración de aplicabilidad y la implementación de controles.		

<table>
<tr><td colspan="4">Datos del antecedente 03: Nacionales</td></tr>
<tr><td>Título</td><td>Propuesta de aplicación web para mejorar la gestión de auditoría informática en la empresa Calzado Atlas S.A.</td><td>Metodología</td><td>Holístico</td></tr>
<tr><td>Autor</td><td>Chauca Huaman, Clarel Ramiro</td><td>Tipo</td><td>Proyectiva</td></tr>
<tr><td>Año</td><td>2017</td><td>Enfoque</td><td>Cuantitativo - cualitativo</td></tr>
<tr><td>Objetivo</td><td>Diagnosticar la situación actual de la gestión de auditorías informáticas en la empresa Calzado Atlas S.A.</td><td>Diseño</td><td>No experimental</td></tr>
<tr><td rowspan="6">Resultados</td><td rowspan="6">Como resultado al aplicar la propuesta de una aplicación web para la gestión de auditorías informáticas, se podrá ahorrar costos de incidentes, prevenir posibles escenarios de una manera más eficiente que impactan en la continuidad del negocio.</td><td>Método</td><td></td></tr>
<tr><td>Población</td><td>15 colaboradores</td></tr>
<tr><td>Muestra</td><td></td></tr>
<tr><td>Unidades informantes</td><td></td></tr>
<tr><td>Técnicas</td><td>Entrevista</td></tr>
<tr><td>Instrumentos</td><td>Guía de entrevista</td></tr>
<tr><td>Conclusiones</td><td>Se concluye que la propuesta de un aplicativo web para la gestión de las auditorías informáticas para la empresa Calzado Atlas S.A. es viable luego del análisis económico, análisis de ahorro en gasto de incidentes del área de TI y análisis de rentabilidad, como solución informática para la necesidad que presenta.</td><td>Método de análisis de datos</td><td>se utilizó para el tratamiento de la información el programa estadístico de análisis cuantitativo el SPSS 22 y se obtendrán medidas de frecuencia. Así mismo, se utilizó el método de triangulación y categorización. Y para la aplicación de juicios de expertos de la investigación, se realiza a través panel de expertos.</td></tr>
<tr><td>Redacción final al estilo artículo</td><td colspan="3">Chauca Huaman (2017) demostró que la propuesta de un aplicativo web para la gestión de las auditorías informáticas para la empresa Calzado Atlas S.A. es viable luego del análisis económico, análisis de ahorro en gasto de incidentes del área de TI y análisis de rentabilidad, como solución informática para la necesidad que presenta.</td></tr>
</table>

Datos del antecedente 04: Nacionales			
Título	IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE IDENTIDADES PRIVILEGIADAS PARA EL CONTROL DE ACCESO EN UNA EMPRESA DE RETAIL	Metodología	PDCA.
Autor	LUCÍA ASTRID CONTRERAS PÉREZ, ROBERTO ANTONIO VEGA ORTEGA	Tipo	
Año	2019	Enfoque	
Objetivo	Como objetivo es mejorar la gestión de identidades privilegiadas de los administradores de las plataformas de TI en la empresa de retail.	Diseño	
Resultados	Como resultado, se presenta la planificación que garantiza el correcto funcionamiento de la solución Privileged Access Manager. La cual permite disminuir el riesgo interno de seguridad informática con los activos de TI y tiene la trazabilidad de todas las actividades realizadas por los administradores del área de redes, seguridad y base de datos de la empresa.	Método	
		Población	Usuarios con cuenta privilegiadas
		Muestra	
		Unidades informantes	
		Técnicas	Encuesta
		Instrumentos	Guía de encuesta
Conclusiones	En conclusión, Mitigación del riesgo de extracción de información de los activos de TI por usuarios no autorizados, teniendo una administración de accesos basado en roles.	Método de análisis de datos	
Redacción final al estilo artículo	CONTRERAS PÉREZ, VEGA ORTEGA (2019) demostraron que se presenta la planificación que garantiza el correcto funcionamiento de la solución Privileged Access Manager. La cual permite disminuir el riesgo interno de seguridad informática con los activos de TI y tiene la trazabilidad de todas las actividades realizadas por los administradores del área de redes, seguridad y base de datos de la empresa.		

<table>
<tr><td colspan="4">Datos del antecedente 05: Nacionales</td></tr>
<tr><td>Título</td><td>IMPLEMENTACIÓN DEL SOFTWARE LOG360 PARA EL CUMPLIMIENTO DEL REQUERIMIENTO 10 DEL ESTÁNDAR DE SEGURIDAD DE DATOS PARA LA INDUSTRIA DE TARJETA DE PAGO</td><td>Metodología</td><td>PDCA, GAP</td></tr>
<tr><td>Autor</td><td>LAVADO SARMIENTO, DAVID ARMANDO</td><td>Tipo</td><td></td></tr>
<tr><td>Año</td><td>2019</td><td>Enfoque</td><td></td></tr>
<tr><td>Objetivo</td><td>Disminuir las brechas identificadas por medio de la implementación de un software SIEM, como control de seguridad seleccionado, para el acatamiento de la exigencia 10 de la norma PCI DSS.</td><td>Diseño</td><td></td></tr>
<tr><td rowspan="6">Resultados</td><td rowspan="6">Como resultado, la banca es uno de los sectores económicos que más importancia debe darle a la seguridad informática. Esto se debe a que el banco ya tiene implementado otros estándares como la ISO/IEC 27001 y Ley de Protección de Datos (Ley N° 29733), los cuales coinciden con algunos requerimientos de la norma PCI DSS. Por lo que este estándar no reemplaza, los ya implementados, si no, los complementa para darle más seguridad a la organización.</td><td>Método</td><td></td></tr>
<tr><td>Población</td><td></td></tr>
<tr><td>Muestra</td><td></td></tr>
<tr><td>Unidades informantes</td><td></td></tr>
<tr><td>Técnicas</td><td>Encuesta</td></tr>
<tr><td>Instrumentos</td><td>Guía de encuesta</td></tr>
<tr><td>Conclusiones</td><td>En consecuencia, Se automatiza el proceso de auditoría de usuarios con accesos privilegiados, reduciendo considerablemente el tiempo de ejecución. Al eliminar el elemento humano, podemos garantizar el funcionamiento correcto y efectivo del control de seguridad, como también, reducir el costo general relacionado con la realización del proceso de auditoría.</td><td>Método de análisis de datos</td><td></td></tr>
<tr><td>Redacción final al estilo artículo</td><td colspan="3">LAVADO SARMIENTO (2019), evidenció que la banca es uno de los sectores económicos que más importancia debe darle a la seguridad informática. Esto se debe a que el banco ya tiene implementado otros estándares como la ISO/IEC 27001 y Ley de Protección de Datos (Ley N° 29733), los cuales coinciden con algunos requerimientos de la norma PCI DSS. Por lo que este estándar no reemplaza, los ya implementados, si no, los complementa para darle más seguridad a la organización.</td></tr>
</table>

8. Marco conceptual

<table>
<tr><th colspan="6">Variable o categoría 1: Seguridad Informática</th></tr>
<tr><th>Autor/es</th><th>Año</th><th>Cita</th><th>Parafraseo (1)</th><th>Aplicación en su tesis (2)</th><th>Redacción final (1+2+3+4)</th></tr>
<tr><td>Proaño Escalante, Rodrigo Arturo,

Gavilanes Molina, Andrés Fernando</td><td>2018</td><td>Garantizar la seguridad de la información, los sistemas de información, servicios y redes implica socializar, también conocer cómo responder ante un evento donde se ha vulnerado dicha seguridad informática y cómo gestionar la evidencia digital identificada, fruto de una vulnerabilidad de seguridad informática. (Proaño, Gavilanes, 2018, p90)</td><td>Para poder brindar una buena seguridad informática y evitar su vulnerabilidad, es necesario una buena gestión, un buen sistema de información, servicio y redes ya que todos estos nos permitirán identificar si es que existe alguna irregularidad en la seguridad informática.</td><td>Para obtener la evidencia digital necesaria se empleará la guía metodológica, esta nos permitirá realizar un proceso en la cual no se comprometerá la confidencialidad e integridad y se llevará a cabo con la norma ISO/IEC 27037 (2012), esta misma menciona que la cadena de custodia ocupa un papel muy importante en la investigación, además hace referencia que se debe saber y comprender cada paso que se realiza en el mano de las pruebas digitales, en consecuencia se brinda una correcta confidencialidad y credibilidad del proceso, teniendo así una custodia limpia y sin negligencias.</td><td rowspan="4">Para poder brindar una buena seguridad informática y evitar su vulnerabilidad, es necesario una buena gestión, un buen sistema de información, servicio y redes ya que todos estos nos permitirán identificar si es que existe alguna irregularidad en la seguridad informática. La Open Source Security Testing Methodology Manual (OSSTMM) es una metodología que usa como base el testeo manual que busca reducir las limitaciones que puedan presentarse entre los activos de información que se buscan proteger y las posibles porosidades de seguridad informática. La seguridad informática es imprescindible ya que este asegura la disponibilidad, privacidad e integridad de la información, para esto existe diversas técnicas, siendo una de ellas la criptografía la cual consiste en transformar un mensaje descifrado que con la ayuda de claves podrá ser descifrado. El sistema de información ha ido evolucionando desde sus inicios, requiriendo la formación de profesionales responsables de evaluar un correcto funcionamiento en el área de informática, así mismo buscan identificar los puntos débiles que necesiten aplicar medidas preventivas y correctiva para así reducir las probabilidades de una perdida de información, tomando en cuenta que estas pérdidas causan costos importantes en la organización. La seguridad informática hoy en día es de suma importancia para las compañías, organizaciones, establecimientos privadas y públicas; de tal manera que el uso de esta ha llegado a incluir diversas actividades profesionales y humanas al nivel mundial ya que las redes de comunicación y los sistemas de comunicación ayudan al crecimiento social y económico de las naciones (Proaño, Gavilanes, 2018; Gordón, Pacheco, 2018; Solís, Pinto, Solís, 2017; Tirado, Álvarez, Carreño, Ramos, 2017; Gil, Gil, 2017).</td></tr>
<tr><td>Referencia:</td><td colspan="4">(Proaño & Gavilanes, 2018)</td></tr>
<tr><th>Autor/es</th><th>Año</th><th>Cita</th><th>Parafraseo (3)</th><th>Aplicación en su tesis (4)</th></tr>
<tr><td>Gordón Revelo, Diego Sebastián,

Pacheco Villamar, Rubén</td><td>2018</td><td>La metodología OSSTMM propone para la optimización de la seguridad de los activos de información, que se disminuyan las limitaciones entre activos de información a proteger y posibles brechas de seguridad, así como también, la no separación de activos de información y brechas de seguridad informática (Gordón, Pacheco, 2018, p15).</td><td>La Open Source Security Testing Methodology Manual (OSSTMM) es una metodología que usa como base el testeo manual que busca reducir las limitaciones que puedan presentarse entre los activos de información que se buscan proteger y las posibles porosidades de seguridad informática.</td><td>Aplicando la metodología OSSTMM y Ethical Hacking, se dispone en la verificación para estimar el impacto y criticidad de las vulnerabilidades halladas, además se medirán los riesgos de la seguridad informática que se encuentran en los canales de información usando la metodología ya antes mencionada y herramientas apropiadas para evaluar la seguridad operacional, por ejemplo: los factores humanos, factores físicos, redes</td></tr>
</table>

				inalámbricas, servicios, aplicaciones, y redes de datos.	Para obtener la evidencia digital necesaria se empleará la guía metodológica, esta nos permitirá realizar un proceso en la cual no se comprometerá la confidencialidad e integridad y se llevará a cabo con la norma ISO/IEC 27037 (2012), esta misma menciona que la cadena de custodia ocupa un papel muy importante en la investigación, además hace referencia que se debe saber y comprender cada paso que se realiza en el mano de las pruebas digitales, en consecuencia se brinda una correcta confidencialidad y credibilidad del proceso, teniendo así una custodia limpia y sin negligencias. Aplicando la metodología OSSTMM y Ethical Hacking, se dispone en la verificación para estimar el impacto y criticidad de las vulnerabilidades halladas, además se medirán los riesgos de la seguridad informática que se encuentran en los canales de información usando la metodología ya antes mencionada y herramientas apropiadas para evaluar la seguridad operacional, por ejemplo: los factores humanos, factores físicos, redes inalámbricas, servicios, aplicaciones, y redes de datos. Con la seguridad informática se deberá mejorar los procesos para un intercambio seguro de información, para obtener este resultado se deberá combinar diversas técnicas como por ejemplo la esteganografía el cual se encarga de ocultar mensajes u objetos dentro de otras llamadas portadores para ser enviada, a su vez hace uso de la criptografía. De la misma forma, se debe acelerar los procesos en los cifrados y descifrados, lo que implicaría una mayor seguridad en menor tiempo. De la misma manera, en el área de TI con el profesionalismo del personal evaluarán el correcto funcionamiento del sistema de información para que los ataques con botnetes no sean introducidos al sistema, así los hackers no tomen control remoto, de esta manera no se convierta la principal amenaza para la red de datos de la empresa. Las Organizaciones contaran con un plan que guíe los esfuerzos de protección de información, deberán aprender a determinar la calidad óptima de inversión en seguridad informática, así desarrollará modelos de
Referencia:	(Gordón & Pacheco, 2018)				
Autor/es	**Año**	**Cita**	**Parafraseo (5)**	**Aplicación en su tesis (6)**	
Solís Fernando, Pinto Diego, Solís Santiago	2017	La seguridad informática cumple un papel muy importante para garantizar la disponibilidad, privacidad e integridad de la información, una de las técnicas que ayuda en esta tarea es la criptografía, cuyo fundamento es transformar un mensaje de modo que sea inentendible salvo para los que posean la clave para descifrarlo. (Solís, Pinto, Solís, 2017, p160)	La seguridad informática es imprescindible ya que este asegura la disponibilidad, privacidad e integridad de la información, para esto existe diversas técnicas, siendo una de ellas la criptografía la cual consiste en transformar un mensaje descifrado que con la ayuda de claves podrá ser descifrado.	Con la seguridad informática se deberá mejorar los procesos para un intercambio seguro de información, para obtener este resultado se deberá combinar diversas técnicas como por ejemplo la esteganografía el cual se encarga de ocultar mensajes u objetos dentro de otras llamadas portadores para ser enviada, a su vez hace uso de la criptografía. De la misma forma, se debe acelerar los procesos en los cifrados y descifrados, lo que implicaría una mayor seguridad en menor tiempo.	
Referencia:		(Solís, Pinto, & Solís, 2017)			
Autor/es	**Año**	**Cita**	**Parafraseo (7)**	**Aplicación en su tesis (8)**	
Álvarez Morales, Elsa Leuvany Carreño Sandoya, Stalin Daniel Tirado Ríos, Normandi Rocío Ramos Reyes, Dorys Janeth	2017	La evolución de los sistemas de información hace necesaria el surgimiento de profesionales en el área informática responsables de evaluar su correcto funcionamiento, detectar aquellos puntos débiles que requieran de medidas preventivas y correctivas para evitar pérdidas de información que podrían	El sistema de información ha ido evolucionando desde sus inicios, requiriendo la formación de profesionales responsables de evaluar un correcto funcionamiento en el área de informática, así mismo buscan identificar los puntos débiles que necesiten aplicar medidas preventivas y correctiva para así reducir las probabilidades de una perdida de información,	En el área de TI con el profesionalismo del personal evaluarán el correcto funcionamiento del sistema de información para que los ataques con botnetes no sean introducidos al sistema, así los hackers no tomen control remoto, de esta manera no se convierta la principal amenaza para la red de datos de la empresa.	

		causar costes importantes a las organizaciones. (Tirado, Álvarez, Carreño, Ramos, 2017, p462)	tomando en cuenta que estas pérdidas causan costos importantes en la organización.		simulación que permitan evaluar el nivel óptimo de seguridad
Referencia:	(Álvarez, Carreño, Tirado, & Ramos, 2017)				
Autor/es	**Año**	**Cita**	**Parafraseo (9)**	**Aplicación en su tesis (10)**	
Gil Vera Víctor Daniel Gil Vera Juan Carlos	2017	En los últimos años, el uso de la informática se ha extendido a la mayoría de actividades profesionales y humanas a nivel mundial. Las redes de comunicación y los sistemas de información (SI) se han convertido en un factor esencial para el desarrollo económico y social de las naciones. Debido a lo anterior, garantizar la seguridad de la información se ha convertido en una tarea de vital importancia y preocupación para empresas, organizaciones e instituciones públicas y privadas. (Gil, Gil, 2017, p193)	La seguridad informática hoy en día es de suma importancia para las compañías, organizaciones, establecimientos privadas y públicas; de tal manera que el uso de esta ha llegado a incluir diversas actividades profesionales y humanas al nivel mundial ya que las redes de comunicación y los sistemas de comunicación ayudan al crecimiento social y económico de las naciones.	Las Organizaciones contaran con un plan que guíe los esfuerzos de protección de información, deberán aprender a determinar la calidad óptima de inversión en seguridad informática, así desarrollará modelos de simulación que permitan evaluar el nivel óptimo de seguridad	
Referencia:	(Gil & Gil, 2017)				

9. Construcción de la categoría problema

Categoría: Seguridad informática					
Criterios	**Fuente 1**	**Fuente 2**	**Fuente 3**	**Fuente 4**	**Fuente 5**
Cita textual	Garantizar la seguridad de la información, los sistemas de información, servicios y redes implica socializar, también conocer cómo responder ante un evento donde se ha vulnerado dicha seguridad informática y cómo gestionar la evidencia digital identificada, fruto de una vulnerabilidad de seguridad informática. (Proaño, Gavilanes, 2018, p90)	La metodología OSSTMM propone para la optimización de la seguridad de los activos de información, que se disminuyan las limitaciones entre activos de información a proteger y posibles brechas de seguridad, así como también, la no separación de activos de información y brechas de seguridad informática. (Gordón, Pacheco, 2018, p15)	La seguridad informática cumple un papel muy importante para garantizar la disponibilidad, privacidad e integridad de la información, una de las técnicas que ayuda en esta tarea es la criptografía, cuyo fundamento es transformar un mensaje de modo que sea inentendible salvo para los que posean la clave para descifrarlo. (Solís, Pinto, Solís, 2017, p160)	La evolución de los sistemas de información hace necesaria el surgimiento de profesionales en el área informática responsables de evaluar su correcto funcionamiento, detectar aquellos puntos débiles que requieran de medidas preventivas y correctivas para evitar pérdidas de información que podrían causar costes importantes a las organizaciones. (Tirado, Álvarez, Carreño, Ramos, 2017, p462)	En los últimos años, el uso de la informática se ha extendido a la mayoría de actividades profesionales y humanas a nivel mundial. Las redes de comunicación y los sistemas de información (SI) se han convertido en un factor esencial para el crecimiento social y económico de las naciones. Debido a lo anterior, garantizar la seguridad de la información se ha convertido en una tarea de vital importancia y preocupación para empresas, organizaciones e instituciones públicas y privadas. (Gil, Gil, 2017, p193)
Redacción de la <u>categoría de estudio</u>	La seguridad de la informática de una empresa cumple un papel muy importante para garantizar la privacidad e integridad de la información y se requiere de profesionales en el área informática responsables de evaluar su correcto funcionamiento.				

Construcción de las sub categorías según la fuente elegida	Sub categoría 1:		Sub categoría 2:	
	Privacidad de la información		**Responsabilidad en el funcionamiento de la información**	
Construcción de los indicadores	I1	Habeas Data	I5	Seguridad de información
	I2	Análisis e identificación de los riesgos	I6	Mantenimiento
	I3		I7	OUTSOURCING
	I4		I8	
Cita textual de la sub categoría	Cuando se hace referencia a la privacidad, se refiere a que la misma queda vulnerada en materia de datos personales, ya que estos se han convertido en elementos o dispositivos de control en una sociedad informatizada y es preciso ser conscientes de por qué y para qué deben protegerse (SOTO, 2017 p.113).		Un Sistema de Gestión de Seguridad de la Información (SGSI) consiste en políticas, procedimientos, directrices, recursos asociados y actividades, gestionadas colectivamente por una organización, en la búsqueda de la protección de sus activos de información. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio. Se basa en la evaluación del riesgo y los niveles de aceptación del riesgo de la organización, diseñada para tratar y gestionar los riesgos de manera efectiva. Analizar requisitos para la protección de los activos de información aplicar los controles adecuados para garantizar su protección, según sea necesario, contribuye a la implementación exitosa de un SGSI (ISO/IEC 27000: 2014 - 3.2.1).	
	Lo que es privado o público se difumina en ocasiones y lo que creemos que es compartido por un número muy reducido de amigos puede ser difundido a un número incalculable de personas durante un tiempo indefinido y de forma peligrosamente descontextualizada (Gregorio & Ornelas 2011 p.196).		Un sistema de gestión utiliza un marco de recursos para lograr los objetivos de una organización. El sistema de gestión incluye la estructura organizativa, políticas, planificación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos (ISO/IEC 27000: 2014 - 3.2.5).	
	Para que una información de un usuario se considere privada debe existir un estricto control sobre su procesamiento. En este sentido, los datos personales en las redes sociales se suelen incluir de una forma sistematizada que pone en peligro la privacidad del usuario al perder control sobre sus datos que pueden ser copiados o transferidos. Evidentemente, en el marco de un mundo digital no se cuentan con las barreras propias de un mundo físico y real que limita en mayor medida el flujo de información que se transmite (Romero 2017 p.10).		Esto se logra mediante la implementación de un conjunto aplicable de controles, seleccionados a través del proceso de gestión de riesgos y administrados utilizando un SGSI; incluye las políticas, procesos, procedimientos, estructuras organizacionales, software y hardware para proteger los activos de información identificados. Estos controles deben ser especificados, implementados, monitoreados, revisados y mejorados, para asegurar que se cumplen los objetivos específicos de seguridad de información y del negocio son logrados. Se espera que los	

		controles de seguridad de la información relevantes se integren a la perfección con los procesos de negocio de la organización (ISO/IEC 27000: 2014 - 3.2.3).
Parafraseo	Al hablar de la privacidad de cierta información, se puede mencionar que esta queda expuesta, por lo tanto, es vulnerable y se va convirtiendo en elementos o dispositivos para un control total que es manejada por ciertas sociedades que van en aumento, así mismo ellas determinan ser consciente de salvaguardar su información.	Al referirnos a un sistema de gestión de seguridad de la información (SGSI) es necesario mencionar que está compuesto por políticas, procedimientos, directrices, recursos asociados y actividades con la finalidad de proteger los activos de información que la organización posee, al mencionar el SGSI hablamos de un enfoque sistemático el cual busca establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información ya que esta es necesaria para que las organizaciones puedan alcanzar sus objetivos de negocio, así mismo se puede indicar que la base para un buen SGSI es la evaluación de los riesgos y los diversos niveles de aceptación ante estos, a su vez es creada para tratar y gestionar de manera correcta los riesgos que surjan en la organización.
	Considerando entre lo personal, o público existe un margen en el que hay ciertas fugas de información porque en muchos casos esta la poseen una pequeña cantidad de personas, sin embargo, esta puede ser difundido a un gran número de personas, siendo así muy riesgoso.	El sistema de gestión está compuesto por una estructura organizativa, políticas, planificación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos, así mismo se puede indicar que el sistema de gestión conoce los recursos que guiaran o ayudaran a lograr los objeticos de la organización.
	Para que los datos personales o cualquier información privada estén protegidas deben cumplir con un estricto control de procesamiento, por ejemplo: los datos personales en las redes sociales cuentan con una sistematización en la que muchos casos esta pone en riesgo la privacidad del usuario, puesto que al insertar esta información se pierde el control facilitando esto a que los datos puedan ser duplicados o transferidos, ello se debe a la falta de límites en el mundo digital.	Para lograr la responsabilidad en el funcionamiento de la información es necesario implementar ciertos controles que han sido elegido por medio de un proceso de gestión de riesgos a través de un SGSI, la finalidad de los controles asegure que se cumplan con los objeticos específicos para poder asegurar la información que posee la información.
Evidencia de la referencia utilizando Ms Word	(Soto, 2017) (Gregorio & Ornelas, 2011) (Romero, 2017)	(ISO/IEC 27000: 2014 - 3.2.1) (ISO/IEC 27000: 2014 - 3.2.5) (ISO/IEC 27000: 2014 - 3.2.3).

Redacción final	Según (SOTO, 2017; Gregorio & Ornelas 2011; Romero 2017)., la privacidad de la información en muchas ocasiones es vulnerada por diversas sociedades que van en aumento, esto se debe a que la información brindada sea utilizada como un elemento o dispositivo por la cual tienen un control total para el manejo de esta, por ejemplo: al registrar los datos personales en una red social se pierde el control absoluto de dicha información es por ello que existe la probabilidad que sea filtrada, duplicada o transferida. Así mismo tomando en consideración lo personal o publico existen ciertos márgenes en lo que se evidencia la fuga de información, esta información puede ser manejada por pequeñas cantidades de personas, sin embargo, estas serían responsables de difundirlas a un gran número de personas siendo este, un riesgo. Por último, se puede indicar que todo esto se debe a la falta de límites en el mundo digital por lo tanto es necesario que los datos personas o cualquier tipo de información privada cumpla con un riguroso control de procesamiento.	Al referirnos a un sistema de gestión de seguridad de la información (SGSI) es necesario mencionar que está compuesto por políticas, procedimientos, directrices, recursos asociados y actividades con la finalidad de proteger los activos de información que la organización posee, al mencionar el SGSI hablamos de un enfoque sistemático el cual busca establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información ya que esta es necesaria para que las organizaciones puedan alcanzar sus objetivos de negocio, así mismo se puede indicar que la base para un buen SGSI es la evaluación de los riesgos y los diversos niveles de aceptación ante estos, igualmente es necesario implementar ciertos los controles asegure que se cumplan con los objeticos específicos para poder asegurar la información que posee la información, a su vez es creada para tratar y gestionar de manera correcta los riesgos que surjan en la organización, además se puede indicar que el sistema de gestión conoce los recursos que guiaran o ayudaran a lograr los objeticos de la organización (ISO/IEC 27000: 2014 - 3.2.1; ISO/IEC 27000: 2014 - 3.2.5; ISO/IEC 27000: 2014 - 3.2.3).

10. Matriz del método

Enfoque de investigación: cualitativo	
Criterios	**Fuente 1**
Cita textual	Utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación. El enfoque cualitativo también se guía por áreas o temas significativos de investigación. Sin embargo, en lugar de que la claridad sobre las preguntas de investigación e hipótesis preceda a la recolección y el análisis de los datos (como en la mayoría de los estudios cuantitativos), los estudios cualitativos pueden desarrollar preguntas e hipótesis antes, durante o después de la recolección y el análisis de los datos (Hernández, Fernández, & Baptista, 2014 p.7).
Parafraseo	El enfoque cualitativo es aquel que utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación (Hernández, Fernández, & Baptista, 2014).
Evidencia de la referencia utilizando Ms word	(Hernández, Fernández, & Baptista, 2014)
Utilidad/ aporte del concepto	Este método se aplicó porque se entrevistó al personal relacionado con el problema de la seguridad informática de una pequeña empresa, y se tomarán sus respuestas como válidas para la investigación.
Redacción final	El enfoque cualitativo es aquel que utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación (Hernández, Fernández, & Baptista, 2014). Este método se aplicó porque se entrevistó al personal relacionado con el problema de la seguridad informática de una pequeña empresa, y se tomarán sus respuestas como váliaprendas para la investigación.

Método de investigación 1: estudio de caso	
Criterios	**Fuente 1**
Cita textual	Estudiamos un caso cuando tiene un interés muy especial en sí mismo. Buscamos el detalle de la interacción con sus contextos. El estudio de casos es el estudio de la particularidad y de la complejidad de un caso singular, para llegar a comprender su actividad en circunstancias importantes (Stake, 1999 p.11).
Parafraseo	El estudio de caso es aquel que investiga, analiza una situación o problemática de manera individual dentro de una sociedad o entidad; así mismo, el lugar donde interactúan diferentes personas, tiene por finalidad de entender su relación (Stake, 1999).
Evidencia de la referencia utilizando Ms word	(Stake, 1999)
Utilidad/ aporte del concepto	Se aplicó en la investigación porque se analiza el problema en particular; en este caso, en una pequeña empresa y sirvió para que esta entidad comprenda las carencias que tiene y que repercuten en la seguridad informática.
Redacción final	El estudio de caso es aquel que investiga, analiza una situación o problemática de manera individual dentro de una sociedad o entidad; así mismo, el lugar donde interactúan diferentes personas, tiene por finalidad de entender su relación (Stake, 1999). Por dicha razón que se aplicó en la investigación porque se analizó el problema en particular; en este caso, en esta pequeña empresa y sirvió para que esta entidad comprenda las carencias que tiene y que afectan en la seguridad informática.

Método de investigación 2: analítico	
Criterios	**Fuente 1**
Cita textual	Este método consiste en la extracción de las partes de un todo, con el objeto de estudiarlas y examinarlas por separado, para ver, por ejemplo, las relaciones entre éstas, es decir, es un método de investigación, que consiste en descomponer el todo en sus partes, con el único fin de observar la naturaleza y los efectos del fenómeno. Sin duda, este método puede explicar y comprender mejor el fenómeno de estudio, además de establecer nuevas teorías (Gomez, 2012 p.16).
Parafraseo	El método analítico consiste en definir la extracción de un elemento en fracciones, de las cuales tiene como objetivo estudiar, examinar de manera individual y aislada; esto es, que se pueda comprender la intercomunicación entre sí (Gomez, 2012).
Evidencia de la referencia utilizando Ms word	(Gomez, 2012)
Utilidad/ aporte del concepto	Se aplicó porque el problema de seguridad informática se observó dentro de la empresa, a través de sus sistemas y a nivel de filtración de datos relacionada con el problema.
Redacción final	El método analítico se define como el estudio de un elemento desmembrado en fracciones, de las cuales se pretende investigar cada una de manera individual y aislada, en tal sentido, que se pueda comprender la interrelación que tienen entre sí (Gomez, 2012).En tal sentido, se aplicó porque el problema de seguridad informática se observó dentro de la empresa, a través de sus sistemas y a nivel de filtración de datos relacionada con el problema.

11. Categorización de la categoría

Sub categoría	Indicador	Ítem
SC1Privacidad de la información	I1Habeas Data	1. ¿Cuál es la situación del Perú con respecto a la Protección de Datos comparado con los países de la Región? 2. ¿Por qué se conoce tan poco la ley de Habeas Data en el Perú?
	I2Análisis e identificación de los riesgos	3. ¿Quién regula el análisis de la Empresa y quién identifica los riesgos de la empresa de los ataques cibernéticos? 4. ¿Encriptas de alguna forma tus bases de datos y la información sobre tus clientes?
SC2Responsabilidad en el funcionamiento de la información	I3Seguridad de información	5. ¿A qué se debe y qué consecuencias tiene para las empresas o entidades del estado? 6. ¿Qué opina, cuáles son los riesgos y las ventajas de las nuevas tecnologías de comunicación?
	I4Mantenimiento	7. ¿Limitas el número de empleados que tienen privilegios de administrador en la infraestructura TI de tu empresa? 8. ¿Quién es responsable de instalar y mantener el software de seguridad en tu computadora?
	I5Outsourcing	9. ¿Por qué las empresas recurren al outsourcing? 10. ¿Qué características se debe tomar en cuenta a la hora de elegir a un outsourcing?

12.- Población, muestra y unidades informantes

Escenario de estudio	
Criterios	
Lugar geográfico	La empresa de Industrias de Alimentos está ubicada en el distrito de San Martin de Porres.
Provincia/Departamento	Lima.
Descripción del escenario vinculado al problema	La empresa en estudio se creó en el año 2010, se dedica a elaborar productos de panificación netamente a programas sociales en Lima y provincias, el servicio que brinda principalmente es el traslado y preparación de alimentos al programa social Qali Warma, y presenta dificultades en el área Administrativo y Logístico lo cual genera un problema con la información.

Participantes					
Criterios	**P1**	**P2**	**P3**	**P4**	**P5**
Género	Masculino	Masculino	Femenino	Masculino	Masculino
Edad	28	30	26	26	30
Profesión/ocupación	Bachiller en Ingeniería de Sistemas / jefe de sistemas	Bachiller en Ingeniería de Sistemas / Analista de proyectos	Bachiller en Ingeniería de Sistemas / Analista de sistemas	Bachiller en Ingeniería de Sistemas / Desarrollador	Técnico en redes y comunicaciones / Asistente de soporte
Tiempo en la empresa	7 años	2 años	2 años	5 años	3 años
Justificar porqué se seleccionó a los sujetos	Todos los participantes fueron seleccionados para esta entrevista, porque están involucrados con el problema que tiene la empresa, asimismo, conocen del problema.				

13. Técnicas e instrumentos

Técnica de recopilación de datos 1 entrevista	
Criterios	**Fuente 1**
Cita textual	La entrevista de investigación es por lo tanto una conversación entre dos personas, un entrevistador y un informante, dirigida y registrada por el entrevistador con el propósito de favorecer la producción de un discurso conversacional, continuo y con una cierta línea argumental, no fragmentada, segmentada, precodificado y cerrado por un cuestionario previo del entrevistado sobre un tema definido en el marco de la investigación (Vargas, 2012 p. 124)
Parafraseo	La entrevista se define como un dialogo abierto que se establece entre dos personas, en el cual el entrevistador es el que guía al entrevistado con el objetivo de obtener información autentica acerca de un tema específico (Vargas, 2012).
Evidencia de la referencia utilizando Ms word	(Vargas, 2012)
Utilidad/ aporte del concepto	Esta técnica aportó a la investigación porque permitió conocer los criterio y opiniones de los involucrados con el problema.
Redacción final	La entrevista se define como un dialogo abierto que se establece entre dos personas, en el cual el entrevistador es el que guía al entrevistado con el objetivo de obtener información autentica acerca de un tema específico (Vargas, 2012). Por tanto, esta técnica aportó a la investigación porque permitió conocer los criterio y opiniones de los involucrados con el problema.

Instrumento de recopilación de datos 1 guía de entrevista	
Criterios	**Fuente 1**
Cita textual	La guía de entrevista no es un protocolo estructurado. Se trata de una lista de áreas generales que deben de cubrirse con cada informante. En la situación de entrevista, el investigador decide cómo enunciar las preguntas y cuándo formularlas. La guía de entrevista sirve solamente para recordar que se deben hacer pregunta sobre ciertos temas. El empleo de guías presupone un cierto grado de conocimiento sobre las personas que uno intenta estudiar. Este tipo de guía es útil cuando el investigador ya ha aprendido algo sobre los informantes a través del trabajo de campo, entrevistas preliminares u otra experiencia directa (Balcázar, González-Arratia, Gurrola, & Moysén, 2013 pp. 63,64)
Parafraseo	La guía de entrevista es un instrumento de recopilación de datos en donde se encuentran las dudas que tiene el entrevistador para efectuar al entrevistado, como resultado, ayuda a documentar y observar el trabajo de campo (Balcázar, González-Arratia, Gurrola, & Moysén, 2013).
Evidencia de la referencia utilizando Ms word	(Balcázar, González-Arratia, Gurrola, & Moysén, 2013)
Utilidad/ aporte del concepto	Sirvió de ayuda a la investigación porque se usará una entrevista como instrumento de recopilador de datos.
Redacción final	La guía de entrevista es un instrumento de recopilación de datos en donde se encuentran las dudas que tiene el entrevistador para efectuar al entrevistado, como resultado, ayuda a documentar y observar el trabajo de campo (Balcázar, González-Arratia, Gurrola, & Moysén, 2013). Por lo tanto, Sirvió de ayuda a la investigación porque se usará una entrevista como instrumento de recopilador de datos
Ficha técnica del instrumento	Nombre: Guía de entrevista para medir el análisis de la seguridad informática. Autor: Martin Cristian Guevara Lunarejo Año: 2020 Subcategorías – ítems/preguntas: SC1 Privacidad de la información (1-4); SC2 Responsabilidad en el funcionamiento de la información (5-10)

	Paralelo entre los instrumentos para la recopilación de datos	
Subcategoría	**Instrumentos**	
	Entrevista	
	Nro	**Item**
Privacidad de la información	**1.**	¿Cuál es la situación del Perú con respecto a la Protección de Datos comparado con los países de la Región?
	2.	¿Por qué se conoce tan poco la ley de Habeas Data en el Perú?
	3.	¿Quién regula el análisis de la Empresa y quién identifica los riesgos de la empresa de los ataques cibernéticos?
	4.	¿Encriptas de alguna forma tus bases de datos y la información sobre tus clientes?
Responsabilidad en el funcionamiento de la información	**5.**	¿A qué se debe y qué consecuencias tiene para las empresas o entidades del estado?
	6.	¿Qué opina, cuáles son los riesgos y las ventajas de las nuevas tecnologías de comunicación?
	7.	¿Limitas el número de empleados que tienen privilegios de administrador en la infraestructura TI de tu empresa?
	8.	¿Quién es responsable de instalar y mantener el software de seguridad en tu computadora?
	9.	¿Por qué las empresas recurren al outsourcing?
	10.	¿Qué características se debe tomar en cuenta a la hora de elegir a un outsourcing?

14. Procedimiento

Paso 1:	Revisión de la literatura o del marco teórico.
Paso 2:	Diseño de instrumentos.
Paso 3:	Recopilación de la información.
Paso 4:	Aplicación de la entrevista.
Paso 5:	Diseño del análisis documental.
Paso 6:	Aplicación del análisis documental.
Paso 7:	Triangulación.
Paso 8:	Redacción del informe final.

15. Análisis de datos

Método de análisis de datos Triangulación	
Criterios	**Fuente 1**
Cita textual	La triangulación es un procedimiento de control implementado para garantizar la confiabilidad entre los resultados de cualquier investigación. Los resultados que han sido objeto de estrategias de triangulación pueden mostrar más fuerza en su interpretación y construcción que otros que han estado sometidos a un único método (Betrián, Galitó, García, Jové, & Macarulla, 2013 p. 6)
Parafraseo	La triangulación es un método de análisis de datos de proceso que busca la integración de distintos datos que permite garantizar los resultados obtenidos evidenciando una explicación más verídica de la investigación (Betrián, Galitó, García, Jové, & Macarulla, 2013)
Evidencia de la referencia utilizando Ms word	(Betrián, Galitó, García, Jové, & Macarulla, 2013)

Utilidad/ aporte del concepto	Ayudó a la investigación porque permitió demostrar la credibilidad de los resultados del análisis de datos.
Redacción final	La triangulación es un método de análisis de datos de proceso que busca la integración de distintos datos que permite garantizar los resultados obtenidos evidenciando una explicación más verídica de la investigación (Betrián, Galitó, García, Jové, & Macarulla, 2013). En este sentido, ayudó a la investigación porque permitió demostrar la credibilidad de los resultados del análisis de datos.

16. Aspectos éticos

APA	En este trabajo de investigación se utilizó la norma APA a fin de evidenciar que no incurrió en algún tipo de plagio, y que la información brindada no fue falseada.
Informantes	Se solicitó la opinión de los informantes y se admitió como válida para la investigación, debido a que tienen vínculo directo con el problema.
Data	El contenido de la data no ha sido modificado ni manipulado a fin de mostrar información veraz y fehaciente.