ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Aplicación de la norma ISO 27009 para prevenir riesgos del sistema de información en la empresa Telefónica, Surquillo

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información

AUTOR:

Br. Luigi Chipulina Puelles (ORCID: 0000-0002-6236-4382)

ASESOR:

Dr. Edwin Alberto Martínez López (ORCID: 0000-0002-1769-1181)

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

LIMA – PERÚ

2020

Dedicatoria

En Memoria de mi segundo padre Saturnino Coapaza Huanacuni quien fue una maravillosa persona, a mis padres quienes con su inmenso amor incondicional han sabido ser ejemplos de valores, entrega unión y esfuerzo y a mi enamorada Chavelita que siempre estuvo en los momentos difíciles de mi vida.

Agradecimiento

Se agradece a mis padres que a pesar de no tener una instrucción académica me han guiado por el buen camino, a mi hermano que siempre tengo su apoyo, a mi enamorada que cuando estuve enfermo y en el proceso de la tesis me apoyo y a mis maestros que gracias a su experiencia me subieron instruir para entregar esta tesis.

Índice

RESUMEN

El objetivo del siguiente trabajo de investigación fue aplicar de la norma ISO 27009 para prevenir los riesgos del sistema de información en la empresa Telefónica, Surquillo, fue necesario la aplicación de esta norma para reducir lo riesgos de seguridad, poder implementar un perímetro de seguridad mas robusto para prevenir la intrusión de personal ajeno al servicio, también actualizara la documentación actual, generando mayor conocimiento por los colaboradores de las distintas empresas, reduciendo así interrupciones laborales y brindando un mejor servicio de calidad, luego de esta aplicación la alta gerencia quedo satisfecha con la reducción de los tiempos de interrupción, seguridad robusta y documentación descriptiva.

El tipo de investigación tuvo un enfoque cualitativo, ya que se usó la observación para tomar la información necesaria, la población que se utilizo para el desarrollo de esta tesis fueron los 3 jefes del área de seguridad quienes brindaron información de su interacción y lo que han podido observar durante su tiempo de trabajo mediante la entrevista brindada, esta investigación será aplicada tecnológica ya que presenta ciertas características que logran vincular de manera natural con la innovación tecnológica, el diseño fue acción por lo que tiene el método de la indagación introspectiva colectiva ya que se emprende por participantes en una situación social que se tiene por objetivo la mejora de la racionalidad.

Se obtuvieron los resultados de mejora de la seguridad de la información donde se redujeron los riesgos informáticos, se obtuvo documentación más robusta y con mejor detalle de las vulnerabilidades, esto se reflejará con la reducción de la interrupción de los usuarios, con esto se concluye que la aplicación de la norma fue necesaria para un mejor servicio y garantía en la seguridad, causando satisfacción y confiabilidad del servicio. Para la aplicación de la norma ISO 27009 se concluyó que se determinó la influencia de la aplicación de la norma para prevenir los riesgos del sistema de información para poder trabajar de una forma más eficiente y segura, la disponibilidad de la aplicación de la norma esto aumento el tiempo de reacción ante un ataque informático, creando parámetros de contingencia capaces de responder, ante alguna incidencia también la confidencialidad del sistema de información esto aumento la seguridad para mantener los datos personales de cada usuario, evitando vulnerar la información privada.

Palabras claves: vulnerabilidad,seguridad,intrusos,interrupción,datacenter.

ABSTRACT

The objective of the following research work was to apply the ISO 27009 standard to prevent the risks of the information system in the Telefónica company, Surquillo, it was necessary to apply this standard to reduce security risks, to implement a more robust security perimeter to prevent the intrusion of non-service personnel, also updating of the current documentation, generating greater knowledge by the collaborators of the different companies, thus reducing labor interruptions and providing a better quality service, after this application senior management was satisfied with reduced interruption times, robust security and descriptive documentation.

The type of research had a qualitative approach, since observation was used to take the necessary information, the population used for the development of this thesis were the 3 heads of the security area who will provide information on their interaction and what they have done. You will be able to observe during your work time through the interview provided, this research will be applied technologically since it will present specific characteristics that will be able to link naturally with technological innovation, the design was action so it has the method of collective introspective investigation since It is undertaken by participants in a social situation that aims to improve rationality.

The results of the improvement of information security were obtained where the computer risks were reduced, more robust documentation was obtained and with the best detail of the vulnerabilities, this was achieved by reducing the interruption of users, with this we conclude that the application of the standard was necessary for a better service and guarantee of safety, causing satisfaction and service reliability. For the application of the ISO 27009 standard, it was concluded that the influence of the application of the standard was determined to prevent the risks of the information system to be able to work in a more efficient and safe way, the availability of the application of the standard increases this The reaction time to a computer attack, creating response trigger contingency parameters, in the event of any incident also the confidentiality of the information system, this increases the security to maintain the personal data of each user, avoiding violating private information.

Keywords: limitations, security, intruders, interruption, datacenter.

I. INTRODUCCIÓN

En el aspecto Internacional según Humphreys (2017) las industrias que brindan un servicio de Infraestructura de TI ISO 27009, explica las normas de seguridad de la información, específica para cada distintivo de la ISO 27009 los requisitos para esta norma incluyen la dependencia de la ISO 27000 para mejorar la efectividad de la ISO 27009. Define cómo incorporar los requisitos y controles referentes a la ISO 27001 se aplican a sectores especificados, obteniendo una secuencia lógica del proceso de las normas. Uno de los casos internaciones más interesantes es de la empresa Telefónica – España, que implemento la normativa ISO 27009 buscando aumentar la seguridad en dicha sede los problemas principales fueron, la falta de falta de seguridad en sus procesos y la falta de visibilidad a mediano y largo plazo, el responsable del ISO SC 27/WG 1, indico que la que la ISO 27009 es la más utilizada para mejorar la seguridad, por lo que la reglamento ISO 27009 optimiza el panorama de la seguridad y brinda las directrices del diseño de la ISO de la seguridad y la información privada mejorando la seguridad. Los trabajadores de Tdp España, ha recibido un aviso que paren su trabajo mediante un ataque ransomware(Es una aplicación que limita el acceso al usuario) , la documentación de contingencia esta desactualizada , ante este ataque la empresa carecía de un protocolo de acción para restringir a estos intrusos este tipo de ataque se ha vuelto común para secuestrar los datos que comprometen a la compañía por la falta de implementación de la ISO 27009.

En el aspecto nacional según Telefónica (2017) La organización comercial de TdP persigue brindar un mejor servicios de calidad a las distintas compañías con tecnología sofisticada y en procesos en recta con la trecho de revolución digital por la que actualmente cruza la empresa, la tecnología más reciente y de mejor calidad de servicio de Telefónica, para mejorar el servicio adquirió diversos certificados y otras normas ISO entre ellas y tenemos ISO 9001:2008 para mejorar la gestión de los procesos de conveniencia y ejecución de las infraestructuras seguras y las redes de telecomunicaciones de Telefónica Perú, el monitoreo ,mantenimiento correctivo y la prevención interna de servicios, Internet, , banda ancha, dial up, datos e interconexión; la ISO 14001 del sistema de gestión del Ambiente para procesos de la instalación de los servicios, mantenimiento, desmontaje y operación de telefónica teniendo como base las tecnologías inalámbricas(Wireless) del último peldaño; y, ISO 27001. para el Sistema de gestión de seguridad, en temas de redes y plataformas. El principal servicio que brinda Telefónica se ejecutaron en el batiente de contratos que fueron

otorgados por el estado, la ley de telecomunicaciones tanto como su estatuto casero, ya que las normas fueron expedidas por este. Los contratos privilegiados de TdP que fueron firmados en 1994 para que se realice la asistencia de los servicios de telefonía sala y de larga jalón doméstico e internacional han sido renovados progresivamente en tres ocasiones, ya que se pudo ampliar el privilegio hasta noviembre del 2027, sucedido en el evento de Telefónica Móviles, los contratos que se realizaron mediante la prestación de servicio de telefonía movedizo en Lima.

La seguridad tanto como la privacidad en internet a llevado a la empresa Telefónica a realizar una investigación de esfera para que se pueda aprender la inducción de los usuarios ante estos temas. Los usuarios dan su calificación en una escala de 0 a 10 y la concurrencia a diversas afirmaciones sobre temas de privacidad el 83,5% ya que reconocen este sinopsis como de gran reputación ya que este le dan como valoración entre 7 y 10 y la mayoría el 55,3 % le dan la valoración de 10, ya que el aforo le da la puntuación como se observa en el resultado 2, además de que la puntuación de 10 es la más común cuando se realiza la pregunta a los usuarios con referencia a la misión que pueda tener una apariencia en poder identificar tanto como obturar la filiación de internet si lo desea y si la obligación de ser aparente se pueda realizar el movimiento de los datos a otra plataforma o red social, con un porcentaje de 65,7% y un porcentaje de 38% que dan resultados de bienestar al momento de la calificación. Realizando la ampliación al cargo de las calificaciones entre 7 y 10, logran indicar que se puede hallar un defensor con respecto a la inscripción ya que se pudo observar que esos dígitos aumentaron en un porcentaje de 85,2% en la primera casualidad y un 62,2% en un instante. Debido al ataque Ransomware sufrido en telefónica España, secuestraron la red interna por ende se perdió gestión de varios servicios, la falta de actualización de normas contribuye a brindarles puertas traseras para que los intrusos vulneren la seguridad y puedan tomar ventaja sobre la empresa.

Es frente a esta realidad que la empresa Telefónica del Perú se dedica a brindar servicios de telecomunicación a grandes empresas como Huawei, Nokia, el Banco continental, entre otros ,actualmente está realizando la modalidad de teletrabajo, debido a la pandemia mundial , por lo que se han logró descubrir algunas vulnerabilidades como la suplantación de identidad, la extorción cibernética, el robo de claves, vulnerabilidad de los sistemas, entre otros , entonces fue imprescindible conocer que no toda la información adquiriere igual nivel de sensibilidad. Es por ello que se obtuvo la información de que, en

condiciones normales el usuario no debió tener problemas al momento de navegar por la web o bajar la información de dichos sitios u obtener las búsquedas que se relacionen con productos, o viajes. Entonces, alguna información que se compartió en Internet cuenta con una sensibilidad que dio como resultado peligroso en el que puedan estar con personas u organizaciones en el cual puedan disponer ilícitamente de ella, ya que en estos grupos cuentan con los datos personales, direcciones o detalles de cuentas bancarias. Finalmente, existieron casos en el que se situaron otras informaciones en el cual se vuelven delicadas como fotos privadas, problemas de salud, etc. Por lo que se presentó el siguiente trabajo de investigación como una alternativa para evitar estos tipos de ataques informantico.

Respecto a los antecedentes internacionales tenemos a Noguera (2019) en su investigación Aplicación de un sistema para detectar intrusos para la empresa Venezolana del vidrio S.A, tuvo como finalidad realizar el análisis de distintos análisis para la plataforma tecnológica ya implementada, es por ello que se realizó un estudio de la realidad problemática con el objetivo de definir un óptimo escenario técnico, entonces se llevó a cabo la aplicación y el correcto desarrollo del resultado tecnológico que permitió amplia todo tipo de capacidades en torno a la seguridad cibernética, cumpliendo con usar las soluciones que todo sw libre necesite, cuya conclusión es detectar los ataques en tiempo real requiriendo análisis activos a través del firewall y los dispositivos de red IDS/IPS. Tuvo como conclusión que reducirá los costos por lo que no se adquirirá algún equipo adicional, se utilizó para detectar la intrusión de personas ajenas al servicio.

Según Ortelli (2018) en su investigación Normativa aplicada en la seguridad informática tuvo como objetivo investigar la gerencia y la problemática que conllevó al tema de la seguridad informática en las diversas organizaciones modernas (Caso de Gandalf Comunicaciones, C.A.), cuya conclusión tomó más conciencia acerca de la seguridad informática, gracias a los ataques recientes que han sufrido grandes empresas transnacionales. Con la aparición de nuevos riesgos, amenazas y vulnerabilidades, obligaran a las organizaciones a solicitar personal altamente capacitado en la seguridad informática, en el cual se pueda permitir conocer sobre las nuevas tecnologías, protocolos y estándares de seguridad disponibles que fueron implementados de acuerdo a las necesidades de la organización. Tuvo como conclusión que se establecerán nuevos parámetros informáticos para predecir las puertas traseras y restringir a los intrusos, mediante análisis continuos.

Según. Heffel (2016) en su investigación sobre seguridad informática en el sector industrial de energía eléctrica tuvo como objetivo principal definir que es seguridad informática, en el sector industrial, así como los detalles inherentes al campo del que se desarrollan las distribuciones de energía eléctrica, ya que estableció relaciones entre los 2 mundos, analizando la realidad problemática, ya que la conclusión después que el autor tuvo conversaciones con diferentes ex empleados de las empresas contratistas de los USA y especialistas en guerra informática digital, asi mismo menciona que tienen las capacidades de dañar el sistema."

Según. Peña (2016) en su investigación diseño e implementación de las redes privadas de vpn, se logrará utilizar el método de la autenticación Idap en la empresa C – Internet S.A ya que tuvo la finalidad de la protección de la conexión de acceso remoto hacia la empresa por intermedio de un contenido cifrado, ya que este pudo asegurar la constancia de la empresa ya que se pudo permitir instaurar la conexión de teniendo diversas ubicaciones geográficas y al emplear el protocolo Ldap en la vpn – ssl se afianzaron en el manejo de la credencial desde el inicio de sesión en Windows hasta los usuarios que utilizan la Vpn. Finalmente, se logró proponer las actualizaciones, renovaciones del licenciamiento tanto como auditorías de la conexión Vpn. Se concluye que este tipo de sincronización VPN es más seguro causando, mayor seguridad ante algún posible intento de infiltración, también para garantizar un mejor servicio se solicitó tener parchado Windows y el antivirus licenciado y actualizado.

Según Rocha (2019) en su investigación titulada modelo de gestión de seguridad informática para el sector público, tuvo como objetivo tener las estrategias tanto como los distintos requerimientos de la seguridad, en el cual se permitió la confidencialidad, integridad y disponibilidad por intermedio de un óptimo uso de los riesgos del cual se expusieron los activos de información, cuya conclusión refirió que existe una disposición de un organismo gubernamental como la (SNAP), que dispuso de la aplicación del Esquema Gubernamental para la seguridad informática, que se basó en el ISO/IEC27001, sin embargo la brecha de implementación es grande debido a que la identificación de activos tangibles tanto como intangibles de las áreas gubernamentales y la determinación de los riesgos amenazas y vulnerabilidades una tarea minuciosa y larga, por lo que la aplicación de un SGSI por procesos estratégicos, de acuerdo a las particularidades anotadas en esta investigación, dio paso a un mejor manejo de la seguridad. Se concluye que gracias a esta

norma de seguridad se evitaran riesgos ante algún ataque informático, se documentaran cualquier incidente de forma eficiente y se tendrá una mejor gestión de seguridad.

Para la fundamentación de nuestra investigación se recurrió a trabajos precedentes que nos permitieron entender el comportamiento de estos dos sistemas independientes. Dentro de los antecedentes nacionales tenemos a Rodríguez (2019) en su investigación: Modelo de la gestión de riesgos en la tecnología informática como soporte en la perseverancia del negocio en una empresa que ofrece un software como un servicio, entonces se tuvo como objetivo un reporte del cual tiene como resultado la motivación hacia los individuos tanto como las organizaciones para que puedan tener el pensamiento en una forma crítica tanto como creativa acerca de cómo dar la respuesta rápida a un medio de riesgo en evolución, cuya conclusión logró que la empresa pueda comprometerse teniendo los esfuerzos en poder realizar la gestión de riesgos como un proceso intrínseco, muy distinto de la gestión inicial diaria que se llevó antes de la aplicación de esta investigación.

Según. Banda (2019) en su investigación: Modelo en metodología de la gestión de riesgos en tecnologías de la información para mejorar la seguridad de los activos informáticos en empresas agroindustriales en Lambayeque. Esta investigación tuvo la metodología que se relacionó con la gestión de riesgos, la misma que se adaptó al rubro del sector agroindustrial ya que proporciona una guía siendo imprescindible para tener como respuesta la reducción del nivel de riesgo, y se concluyó que se contribuye con la mejora de la seguridad informática ya que se logrará desarrollar un modelo que se basó en las metodologías de gestión de riesgos de tecnologías informáticas para empresas que son del rubro agroindustrial en Lambayeque.

Según. García (2018) en su investigación: Modelo de seguridad de la información para el apoyo en la gestión ambiental en Lambayeque, tuvo como finalidad de poder ayudar en la seguridad informática de la gestión de la unidad ambiental en Lambayeque, y se tuvo como propuesta la preparación del modelo de seguridad de la información que se basó en estándares, marcos de trabajo como metodologías que pudieron adaptarse a la gestión de la unidad ambiental, y se concluyó que existen similitud en las opiniones de los especialistas con relación a la claridad, suficiencia, coherencia tanto como relevancia ya que este valor es significativo.

Según Yañez (2018) en su informe de tesis llamado: Sistema de gestión en la seguridad de la información para la subsecretaria de economía, como empresas de menor tamaño en la U. de Chile, tuvo como problema la indicación que no tuvieran las medidas para la protección de la integridad, como confidencialidad, de la información crítica. La seguridad de la información no se trató en forma planeada ya que es responsable de unidades específicas y menos por temas para la organización.

Según Olivares (2016) en su tesis, modelo de la gestión de la seguridad en la información para el e-gobierno, dicha investigación comenzó elaborando un estudio básico, con un diseño no experimental, siendo de corte transversal. Dicha población está formada por varias entidades públicas, así como del mismo tamaño de la muestra. Se elaboró las revisiones de modelos en la seguridad de información basándose en estándares, ya que se definen las empresas como funciones de seguridad, dimensiones de disponibilidad y controles de seguridad de riesgos objetivos estratégicos, ya que se produjeron por distintos incidentes informáticos ya que uno de ellos era la interrupción no concisa y difusión de información sensible. preparando el trabajo de investigación de aplicación de un SGSI que especifica dicha pesquisa ya que se logra un cambio de enfoque.

Según Rodríguez (2016) en su tesis nombrada como: factores que dañan la implementación de un SGSI en entidades públicas peruanas en referencia de la NTP - ISO/IEC 27009, puesto que se realizó un estudio básico, con diseño no experimental y de corte transversal. Este proyecto brindó un sustento para la investigación pública nacional del que se realizó este informe. al final dicha investigación terminó al hacer referencia a la dimensión de dichos análisis de riesgos.

Para implementar ISO 27009 según Dejan Kosutic (2019) mencionó que posiblemente se logre buscar una manera sencilla para realizarlo. Entonces enfatizó: No existe una manera fácil para lograrlo. Sin embargo, se puede intentar dar la facilidad al trabajo, entonces, este es una lista de dieciséis pasos que se tendrá que continuar para poder obtener la certificación ISO 27009: y como parece algo obvio, generalmente no se toma con la seriedad que amerita. Pero, según mi experiencia, el objetivo en la desilusión de los proyectos para lograr la implementación de dicha norma, es decir, no destina suficientes recursos humanos que se pueda trabajar en dicho proyecto ni teniendo suficiente dinero. Este es un tema complicado ya que involucra distintas actividades, a distintas personas y demande varios meses o más. Es decir, si no se logra definir con claridad que se realizará, quién lo

hará, y en que periodo de tiempo tomando como ejemplo la aplicación del proyecto, es posible que nunca se pueda terminar el trabajo.

Según SGSI. (2015) indica que si es una organización de gran tamaño, tal vez se obtenga el poder realizar la implementación de la norma ISO 27001 únicamente en una parte, minimizando de modo importante de esta forma, los riesgos que tiene el proyecto. (Problemas para poder tener la definición del alcance de dicha norma). La política de SGSI es el documento con mayor importancia, no tiene que ser tan detallado, pero se tiene que definir ciertos temas sobre seguridad de la información en la organización. Pero ¿Cuál es el objetivo si no es meticuloso? Es decir, tiene como finalidad que se logre definir la dirección que se desea alcanzar tanto como el poder tener el control. (Política de Seguridad de la información: ¿Qué nivel de detalle se puede tener?

La evaluación de riesgos es la labor más complicada de la investigación para la norma ISO 27001 ya que tuvo como objetivo la definición de las reglas para que se logre la identificación de los activos, las vulnerabilidades, las amenazas, las consecuencias tanto como las probabilidades, como también se logró definir el nivel de aceptación de riesgo. Si las reglas no se lograran definir con exactitud, la persona encargada podría encontrarse en un momento en que puede obtener resultados ineficaces. (Consejos para la evaluación de riesgos de empresas pequeñas). Tuvo como objetivo del resultado del tratamiento de riesgos la reducción de estos del que no se aceptaron. En este procedimiento se redactó un informe sobre la evaluación de los riesgos del que se pueda documentar ya que se tomaron todos los pasos a lo largo del proceso de la evaluación tanto como el tratamiento de riesgos, también tuvo como importancia lograr la aprobación de los riesgos residuales, ya sea en documentos por separado o como parte de la dirección de la Declaración de aplicabilidad.

Al finalizar el proceso de tratamiento de riesgos, se podrá saber con exactitud qué controles del anexo se deben contar ya que existen aproximadamente un total de 114 controles, sin embargo, es probable que no se cuenten con todos. La finalidad de este documento también llamado Dda es de enumerar los controles en su totalidad, también definir de quién puede aplicarse y quién no, se tuvo que definir los motivos de la decisión, los objetivos que se desea lograr con respecto a los controles tanto como la descripción de cómo se logrará su implementación. La declaración de aplicabilidad también es el documento adecuado para conseguir la autorización de la dirección para que se pueda realizar la implementación del SGSI.

Para que se haya logrado la implementación de los cuatro métodos obligatorios tanto como los controles que corresponden, es habitual la tarea más expuesta del proyecto ya que, implicó aplicar nuevas tecnologías, pero, sobre todo, la aplicación de nuevas conductas en la organización. Frecuentemente las nuevas políticas tanto como procedimientos son imprescindibles (teniendo como sentido que el cambio es importante) ya que las personas tienen resistencia al cambio, por consiguiente, la siguiente actividad (capacitación y concienciación) es de suma importancia ya que se puede prevenir los riesgos. Para que se logre la implementación de las nuevas políticas tanto como procedimientos, es primordial brindar la explicación a los empleados del porqué es imprescindible y poder brindar la capacitación para actuar según la respuesta que se espera. La escasez de las actividades es uno de los motivos principales por la derrota del proyecto para que se logre la implementación de la norma ISO 27001.

Este fragmento en el que la norma ISO 27001 se logró transformar en una rutina cotidiana dentro de la organización. La palabra que tuvo mayor importancia es "registros" ya que a los auditores tienen interés por los registros, es decir, que si no cuentan con registros tendrán dificultades para probar que la actividad se haya conseguido en realidad. Pero, sobre todo, los registros son de gran ayuda para uno, ya que con ellos se puede realizar la supervisión de qué sucede o saber en realidad si los trabajadores o proveedores estén ejecutando las tareas según lo solicitado. ¿Qué sucede en nuestro SGSI? ¿Cuántos incidentes tiene? ¿Qué tipo de incidentes tiene? ¿Se efectúan con exactitud todos los procedimientos? Es en este caso en donde se atraviesan los objetivos de control con la metodología de medición, ya que se debe realizar la verificación que si los resultados que se obtuvo logran cumplir con lo que se pudo establecer en los objetivos. En caso contrario no se cumplan, ya es visible que algo está fallando y se deben de implementar medidas correctivas y/o preventivas.

La finalidad de un sistema de gestión es brindar la garantía que lo que tiene error o llamadas también "no conformidades" sea arreglado o se logre evitar. Por consiguiente, la norma ISO 27001 solicita que las medidas preventivas tanto como correctivas se logren aplicar ordenadamente, en otros términos, se logre identificar la raíz de no conformidad y se logre solucionar tanto como controlar. Según ISO/IEC 27009 dice TI – Técnica de seguridad – Implementación específica por sector de la norma ISO/IEC 27001 – Requisitos para la unión de la familia de normas ISO/IEC 27000 para contribuir a incrementar la eficiencia de

la ISO/IEC 27001 del cual es aplicable a un sector específico, ya que permite que se logre tener una coherencia para el progreso de normas en esta familia ya que asume que todas las condiciones del estándar ISO/IEC 27001 que no se refinan o interpretan, y todos los controles en el estándar ISO/IEC 27002 que no se modifican, se aplicarán en el contexto específico del sector sin cambios.

Humphreys (2016) "Se determina la idea de seguridad de la información como "Esta norma ofrece una protección más a medida para sectores específicos (por ejemplo, las finanzas el transporte y el cuidado de la salud, y proyectos de infraestructura, como las ciudades inteligentes) para protegerse de amenazas a la información, habiéndose convertido en una política comercial además de un imperativo económico, conduciendo la necesidad de normas cibernéticas específicas a cada sector. La recientemente publicada ISO/IEC 27009 ayudará a los normalizadores a hacer precisamente eso, proporcionando el asesoramiento y la orientación necesaria sobre cómo crear normas que aplican la ISO/IEC 27001 para los distintos sectores. La norma ISO/IEC 27009 es una solución de mejora continua en base a la cual puede desarrollarse un Sistema de Gestión de Seguridad de la Información (SGSI) que permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros.Por otro lado, también permite establecer los controles y estrategias más adecuadas para eliminar o minimizar dichos peligros. Como ocurre con todas las normas ISO/IEC, la 27009 es un sistema basado en enfoque basado en el ciclo de mejora continua o de Deming. Dicho ciclo consiste, como ya sabemos, en Planificar-Hacer-Verificar-Actuar, por lo que se le conoce también como ciclo PDCA (acrónimo de sus siglas en inglés Plan-Do-Check-Act). Trasladado a las necesidades de un SGSI, el ciclo PDCA planteado por la ISO/IEC 27009 se dividiría en los siguientes pasos, cada uno de ellos ligado a una serie de acciones".

Un SGSI se basa en la ISO 27009, puerto que está fundamentado por lo que se haga, del como analizar las principales amenazas, ya que par que desde ahí se haga un test de evaluación tanto como la planificación de riesgos. Según Gómez (2017) tiene como finalidad que cada riesgo que se identifique con anterioridad queda cubierto y logre pasar su auditoría, la norma ISO 27009 menciona en su última versión ISO/IEC 27009:2020 hasta 113 puntos de control (en la antigua versión del 2005 eran 133), estos 113 controles se dividen por objetivos de gran cantidad ya que cada organización puede añadir más puntos si es que es conveniente, como también puede personalizarlo para que sean adaptados a su

propio Plan de control operacional, sin embargo, se debe tener un lineamiento según pida la norma y todos los controles en el estándar ISO/IEC 27009 que no se modifican, se aplicarán en el contexto específico del sector sin cambios.

Se puede dar como definición un plan de tratamiento de los riesgos o esquema de mejora luego de realizar el análisis, y se logra definir un plan de tratamiento de mejora, en que se den cuenta de los errores que cometen las distintas conclusiones potenciales de riesgos, logrando establecer una criticidad por cada uno de ellos para que así se pueda dar la evaluación con imparcialidad de las distintas amenazas. Existen diversas formas de enfrentar el riesgo. Una organización afronta el riesgo en tres tipos: Eliminando, calmar o trasladar, elimina el riesgo, entonces, si es riesgo es decisivo que llegue a tal punto que exponga a la propia continuidad de la empresa, esta se debe colocar por diversos medios para lograr eliminarlo, para que haya una oportunidad de que verdaderamente se llegase a producir. No es posible mitigarlo ya que no llega eliminar totalmente el riesgo, ya sea por técnica o porque la organización tome la decisión de que no es un riesgo crítico. La empresa puede admitir el riesgo o tener la conciencia que la amenaza para la información existe y se debe tuvo la dedicación a monitorear con la finalidad de tener todo en control. Definitivamente conviene la implementación de las medidas correctivas o preventivas necesarias ya que tiene como finalidad la reducción de la posibilidad del impacto de riesgo. También puede ser otra opción de realizar su traslado, ya que esta se relaciona con la contratación de un tipo de seguro que logre compensar los resultados económicos del deterioro o pérdida de la información. Teniendo el plan de tratamiento que se eligió por la organización, la gestión de riesgos tiene que asegurar a la organización a tener la calma de tener la identificación de los riesgos tanto como los controles, lo cual permite actuar con eficiencia y eficacia ante una materialización.

También menciona que para que se pueda realizar la implementación de un SGSI es primordial que se pueda definir el alcance para lograr la implementación del sistema en la organización. Ya que se tiene en cuenta que hay la existencia de organizaciones que discrepan por el tamaño o por la cantidad de empleados, volumen de información manejada, número de clientes, volumen de activos lógicos y físicos, el total oficinas, etc. Es por ello que es necesario que se determine de cómo se implanta un SGSI, y se tiene como ejemplo que se puede escoger en qué áreas de la organización se quiere implantar el SGSI como primera opción, cuál o en qué casos se pueda determinar si hay ámbitos de la organización

que por las características que se mencionan no especifican la aplicación de un protocolo de seguridad.

Generalmente, en las primeras áreas se tiene que tener consideración en el cual son aquellas que por las responsabilidades que tienes, brinda apoyo en primera fila a dar cumplimiento a la misión institucional. Se puede tomar como ejemplo la determinación del alcance tanto como privilegiar de una empresa mediana de compra y venta de cosas por Internet y presencialmente en los distintos locales tanto como nacionales, ya que se puede determinar en qué instancia se pueden cubrir áreas de contabilidad, inventariado y facturación y por ser un tema de gran importancia en donde se pueden manejar claves para la empresa, se consideró la logística tanto como atención al cliente, ya que estas áreas permiten un trato directo como los mismos logrando alcanzar la satisfacción esperada tanto como el resto de áreas de las empresas logrando o no incluirse en un principio en el SGSI, para entrar luego de manera violenta y progresiva.

Según Gómez (2017) menciona que el análisis de contexto que tiene la organización es primordial para el sistema de gestión ya que permite decidir la problemática interna tanto como externa de la organización, también sus debilidades, amenazas, fortalezas y oportunidades que nos puede perjudicar. La norma ISO no caracteriza la utilización del método para el análisis del contexto, siendo el método DAFO uno de los más comunes y aceptados. De todos modos, teniendo la elección del sistema que se asigne, es primordial domina la valoración del contexto interno teniendo como base los productos tanto como servicios como los externos teniendo como base logística o clima organizacional.

Según Tarrillo, E. (2016) menciona que se realizó un eficiente análisis de riesgos es por ello que es indispensable poder determinar un contexto de la organización, tener la comprensión de las necesidades tanto como expectativas de las partes interesadas que son los proveedores de los servicios de información y de equipos de tecnologías de la información o también llamados Tics, los clientes ponen un cuidado especial en temas de la protección de la gestión de datos personales, fuerzas de seguridad de cada estado, las autoridades jurídicas para que se pueda tratar los aspectos legales tanto como la participación en foros de índole profesional, la sociedad en general puede identificar los intereses según ISO 27001 ya que no es algo tan complicado.

Según Valencia, H. (2016) mencionó que en necesario tener un aseguramiento de los objetivos para la gestión de riesgos, en el cual pudo ser contables, aunque no es imprescindible que sean contables. Otros de los aspectos es que los objetivos tienen que ser eficientemente anunciados al conjunto de trabajadores de la organización, ya que todos los trabajadores tuvieron que ser conscientes de que contribuyen en una finalidad común, es decir, en un descuido o mala actitud ya que puede ocasionar consecuencias graves. Además de que todas las personas que trabajan en la organización tienen que tener competencias que es imprescindible en temas de seguridad de la información o según la función que se realiza en la empresa. Por otra parte, los objetivos que se definen tienen que estar asociados a ciertos indicadores para que se pueda permitir un seguimiento del cumplimiento de las actividades.

Según Velásquez P, Velásquez S, Velásquez M y Villa J (2017) "La norma ISO/IEC 27009 da mucha importancia a la documentación, estableciendo de manera muy estricta cómo se debe gestionar la documentación y exigiendo que la organización cuente con un procedimiento documentado para gestionar toda la información. Esta cuestión es fundamental para la obtención de la certificación. La documentación puede ser presentada en diversos formatos: documentos en papel, archivos de texto, hojas de cálculo, archivos de vídeo o audio, etc. Pero en cualquier caso constituye un marco de referencia fundamental y debe estar lista en todo momento para que pueda ser consultada. La organización debe gestionar tanto los documentos internos (políticas diversas, procedimientos, documentación del proyecto, etc.), como lo externos (diferentes tipos de correspondencia, documentación recibida con equipamiento, etc.). Por este motivo, la gestión de documentación es una tarea compleja e integral. Con el objetivo de que las empresas gestionen eficazmente los documentos, la norma ISO 27001 exige la aplicación de un método sistemático para su manejo, así como la redacción de un procedimiento para su gestión."

Según Nazareno (2017) mencionó que las definiciones tecnológicas con el transcurrir del tiempo la tecnología logra tener un gran avance de manera rápida ya que se dio a conocer nuevas tecnologías tanto como el equipamiento inevitable para que se pueda enfrentar a los probables ataques o amenazas informáticas en temas de información que tenga manejo la organización. Pero tiene en cuenta que depende de la importancia que la empresa pueda asegurar con respecto a la protección de su información y de mismo modo el costo que pueda destinarse para que se adquiera tanto como renueve el equipamiento como por ejemplo las licencias del software que se encarga de monitorear la red interna de la

empresa que es imprescindible afrontar los ataques que se produzcan. Existen deficiencias en la configuración que el personal técnico de cada organización tiene que realizar una eficiente configuración de los equipos informáticos, ya que esta configuración tiene que estar conectados a la política de accesos personales de los equipos tanto como bloqueos de los accesos que no son autorizados.

Alcalde (2016) pudo establecer que la disponibilidad es de tener acceso a la información en cualquier momento ya que cuando halla retrasos superiores a los establecido según el nivel de servicio puede ser explicado como una violación a la disponibilidad. De este modo si el sistema de información no se encuentra a disposición cuando uno lo requiera es como si no existiera dicho sistema ya que la disponibilidad en mismo modo que otros sistemas que están vinculados a la seguridad de la información se podrían ver afectados por temas técnicos como por ejemplo un mal manejo de una computadora o dispositivo de comunicación, algún fenómeno natural o causas humanas.

Según Moscoso L, Esau E y Soto C (2018), menciona que la información en lucha con la divulgación a las empresas o individuos que no son autorizados ya sean en empresas, personas, maquinas procesos, es decir nadie debe de tener lectura a los datos salvo las empresas que fueron previstas. la integridad con las que cuentas los datos es el resguardo frente a lo que se actualice, duplique o reordene a que es hecho por entidades no autorizadas. Es necesario el uso de la técnica llamada criptográficas. Gestión de Riesgo: Westerman (2016), refiere que la gestión de riesgos en tecnologías de la información tiene un trasfondo en la actualidad ya que se logra evaluar los riesgos técnicos, como también la expansión de riesgos en los diversos niveles que ocasionan pérdidas a la organización o entidad que no tome conciencia de la realización de supervisión del aumento de los niveles de riesgo. Actualmente el jefe que se encarga de una empresa tiende a la valoración de las pérdidas que pudiese generar o brindar una visión económica para que se logre adquirir equipos que reduzcan los riesgos ante los incidentes que puedan afectar la información que pueda manejar la empresa.

Procedimiento de gobierno en temas de riesgo: Según Westerman (2016) están referidas como: “políticas completas y eficaces relacionadas al riesgo, combinado con un proceso maduro y consistente para identificar, evaluar, priorizar y supervisar los riesgos oportunamente, el cual incluye políticas y procedimientos para identificar y evaluar los riesgos y prevenir conductas de riesgo”. Educación sobre riesgos: “Personas cualificadas que

saben cómo identificar y evaluar las amenazas e implementar la mitigación efectiva del riesgo. La conciencia de riesgos ayuda a todos en la empresa a comprender las amenazas y las oportunidades de mitigación".

Para esta investigación se usará una justificación práctica según Laureano y Lorente, (2015) indica que "Las nuevas tecnologías de la información están facilitando un auténtico proceso de cambio empresarial. Consideradas como una mezcla de informática y telecomunicaciones, nos están permitiendo obtener la información necesaria para poder gestionar los nuevos modelos empresariales y conceptos organizacionales. En propósito de un HelpDesk es el establecimiento de un grupo de personas que den soporte a la consecuencia de las tareas del personal contratado.".

Después de lo anterior mencionado tenemos el problema general de investigación: ¿De qué manera influye una Aplicación de la norma ISO 27009 para prevenir riesgos del sistema de información en la empresa Telefónica, Surquillo?, y como problemas específicos: ¿En qué medida una aplicación de la Norma IS0 27009 influye en la disponibilidad de la seguridad de la información?, ¿En qué medida una aplicación de la Norma IS0 27009 influye en la confidencialidad de la seguridad de la información? De esta manera, se plantea el siguiente Objetivo General de la investigación: Determinar la influencia de una aplicación de la norma ISO 27009 para prevenir los riesgos del sistema de información en la empresa Telefónica, Surquillo Y como objetivos específicos: Determinar la influencia de una aplicación de la norma ISO 27009 en la disponibilidad del sistema de información en la empresa Telefónica, Surquillo , Determinar la influencia de una aplicación de la norma ISO 27009 en la confidencialidad del sistema de información en la empresa Telefónica, Surquillo

II. MÉTODO

El problema actual que aqueja es debido al gran avance tecnológico, han evolucionado la forma de engañar a los usuarios y la intrusión de personas no deseadas con el fin de robar, extorsionar, suplantar, entre otras. Para estos casos debemos, además, implementar sistemas de protección perimetral que neutralicen cualquier intento de intrusión de la manera más precoz posible, debido a la peligrosidad del atacante y a las graves consecuencias que sus actos puedan provocar. El estado de seguridad pone en nuestras manos tecnologías como la detección y el análisis de vídeo que, conforme a los parámetros preestablecidos en procedimiento de la necesidad y objetivo del operador, será un eficaz aliado para los elementos de protección.

Esta investigación es cualitativa porque el enfoque que establece va desde lo particular hasta lo general, ya que, a partir de un análisis de una cantidad limitante de datos, el investigador propone conceptos que logren abarcar una explicación completa o describa un fenómeno. Para la fundamentación de nuestra investigación tenemos Mannay (2017) "La investigación cualitativa tiende más hacia la expansión y la generalización del conocimiento y la recolección de los datos al ser documental es mucho más abierta, pues el investigador puede utilizar escritos, entrevistas, material gráfico o audiovisual, siempre que se establezca la pertinencia".

2.1. Tipo y diseño de investigación

Tipo de investigación

Esta investigación será aplicada tecnológica ya que presenta ciertas características que logren vincular de manera natural con la innovación tecnológica, ya que indica que se puede utilizar como un instrumento para impulsar el tema de la innovación. Según Sampieri (2019) "La importancia de la investigación tecnológica es apoyarse en el conocimiento para lograr la transformación de una realidad concreta particular. En el paradigma tecnológico tenemos un proceso que integra la investigación y la transformación a la vez, es decir, requerimos conocer el objeto de estudio para después intervenir en una realidad particular modificando el estado de cosas, hasta alcanzar una aproximación a lo deseado."

Diseño de investigación

Esta investigación – acción tiene el método de la indagación introspectiva colectiva ya que se emprende por participantes en una situación social que se tiene por objetivo la mejora de

la racionalidad tanto como la justicia de las prácticas sociales o educativas. Según O'Hanlon (2019) La investigación-acción tiende a reconocer que el investigador tanto como el participante tienen pensamientos distintos que puede influir en el camino de la investigación. La validez y la autenticidad de la investigación – acción depende de que los que están involucrados sean conscientes de los intereses tanto como los valores personales, ya que dan la forma al propio compromiso.

2.2. Escenario de estudio

El tema de la seguridad se logra determinar como un proceso continuo, tiene que tener la vigilancia tanto como un controlado tratamiento ya que según la norma ISO 27009 menciona que se puede establecer una metodología cuya finalidad es proteger la confidencialidad, integridad como la disponibilidad de la información ya que, en el área de Seguridad de Telefónica, se solicite la aplicación de la metodología para que permita establecer la estrategia de seguridad de la información, teniendo como fin primordial la protección de datos e información utilizando el modelo de mejora continua PHCA(planificar, hacer, controlar y actuar), se inicia con la descripción de SGSI (Sistema de gestión de la seguridad de la información) ya que es donde se logra analizar tanto como definir los escenarios y la planificación (planificar), luego de ello que logra continuar con el progreso del modelo que empieza desde la implementación hasta la ejecución, ya que se determina el control tanto como la aplicación (hacer), en cuanto al tema de SGSI se halla implementado y tiene un buen funcionamiento, ya que comienza el proceso de monitoreo tanto como de revisión (controlar), y finalmente se logra reconocer la mejora que se debe implementar en el sistema (actuar)

2.3. Participantes

Los participantes para la aplicación de esta tesis se consideró a los 3 jefes del área de seguridad de información de Telefónica de surquillo, esta unidad de estudia es considerada por que han sido capacitados por las distintas técnicas y medidas para procesar la información que se mantiene en esta institución y velar que esta información se mantenga privada del sistema de seguridad de información establecida por la empresa Según Baptista, Fernández y Hernández (2017) una población se define como aquel grupo de fenómenos a examinar, donde los entes de la población tienen una particularidad igualitaria a la cual se investiga.

2.4. Técnicas e instrumentos de recolección de datos

Técnicas de recolección de datos

Según Centty Villafuerte (2015), indica que "Son procedimientos metodológicos y sistemáticos que se encargan de operativizar e implementar los métodos de Investigación y que tienen la facilidad de recoger información de manera inmediata, las técnicas son también una invención del hombre y como tal existen tantas técnicas como problemas susceptibles de ser investigados". (p.23)

Instrumentos de recolección de datos

Según Namakforoosh, Mohamad (2016), indica que "la entrevista es empleada en las investigaciones científicas por que consiste en registrar los datos que se van obteniendo llamadas entrevistadas, las cuales, debidamente elaboradas y ordenadas contienen la mayor parte de la información que se recopila en una investigación por lo cual constituye un valioso auxiliar en esa tarea, al ahorrar mucho tiempo, espacio y dinero."

2.5. Procedimiento

Para realización de la presente investigación se tomó en consideración dos fuentes de información: Teórica y de Campo. En la fuente teórica, la información se obtuvo mediante libros, revistas y artículos científicos búsquedas de forma virtual mediante buscadores especializados. En la fuente de campo, los resultados de las entrevistas fueron obtenidos de forma virtual mediante la aplicación de los instrumentos que miden la SGSI (Sistema de Gestión de Seguridad de la Información) y los riesgos.

2.6. Método de análisis de información

Para esta investigación se utilizó el método inductivo ya que mediante este método se logra obtener las conclusiones generales empezando de premisas particulares. Según Vargas (2019) "Se trata de método inductivo, donde en el que pueden distinguirse cuatro pasos esenciales: la observación de los hechos para su registro; la clasificación y el estudio de estos hechos; la derivación inductiva que parte de los hechos y permite llegar a una generalización; y la contrastación. En este sentido, el método inductivo opera realizando generalizaciones amplias apoyándose en observaciones específicas. Esto es así porque en el razonamiento inductivo las premisas son las que proporcionan la evidencia que dota de veracidad una conclusión."

2.7. Aspectos Éticos

dicha tesis toma en cuenta los aspectos técnicos y metodológicos tanto morales como cuando se diseñen los trabajos de investigación. Motivo que dicha tesis cumple con el SGSI, con dicha premisa no se pretende usar ningún dato que vaya contra la empresa, dando una postura diferente que se debe de mejorar y restringir a los users entrar por la fuerza.

III. RESULTADOS

En cuanto a la descripción de resultados, la presente investigación ha efectuado como técnicas de recolección de datos, la entrevista a profundidad con preguntas semiestructuradas, el análisis documental y la observación participante para lograr los objetivos planteados y poder estructurar las respuestas dadas por los expertos consultados. A continuación, se muestran mediante la triangulación de datos la manera como se logra llegar a la conclusión final.

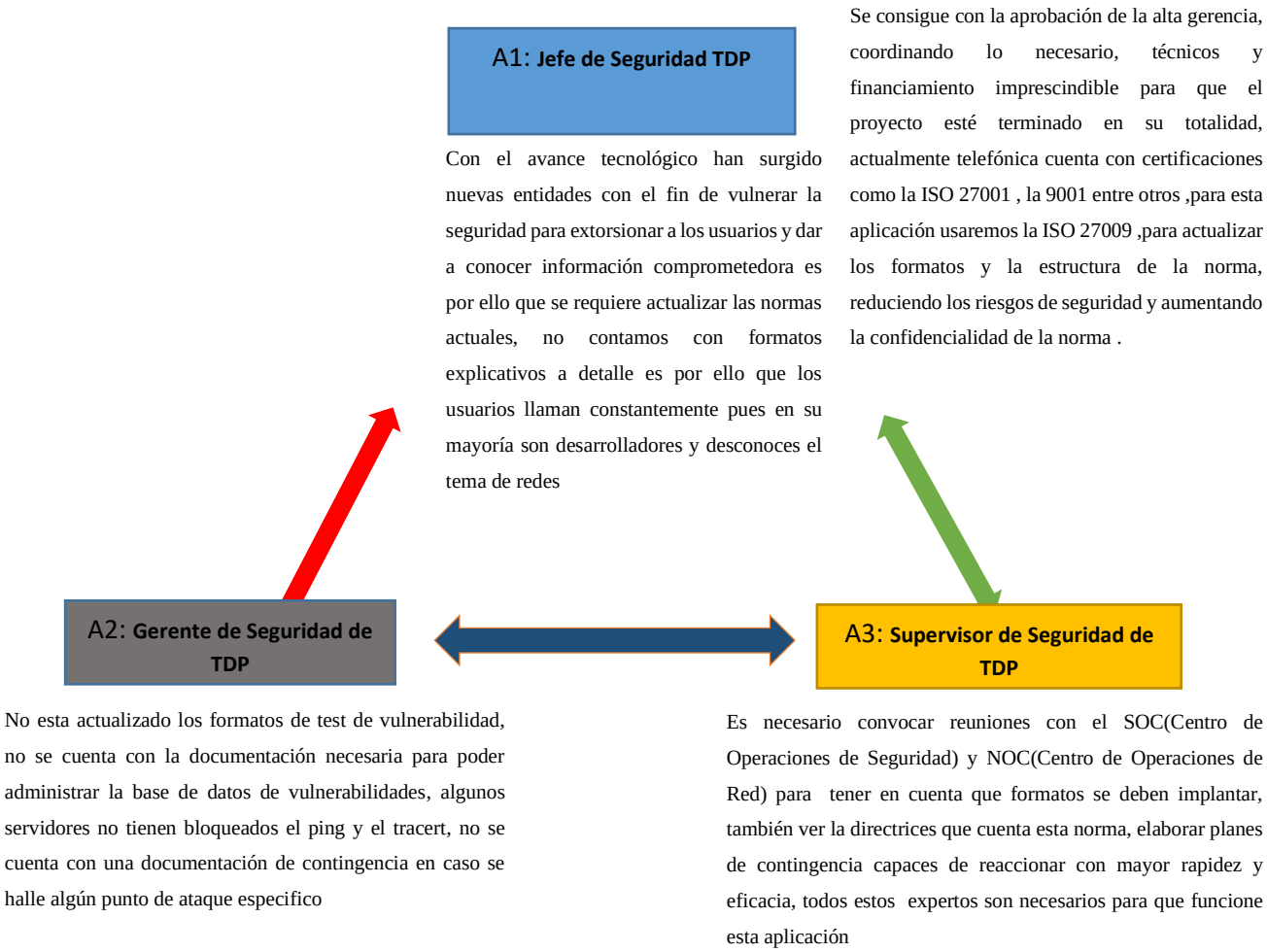

Figura 1: Triangulación de la observación de la unidad de estudio.

De acuerdo con lo presentado se puede concluir que la aplicación de una norma ISO 27009 se tienen que tener el apoyo de las partes involucradas tanto de la alta gerencia, hasta los técnicos encargados, identificando los posibles riesgos de seguridad y los procesos de información de la seguridad.

.

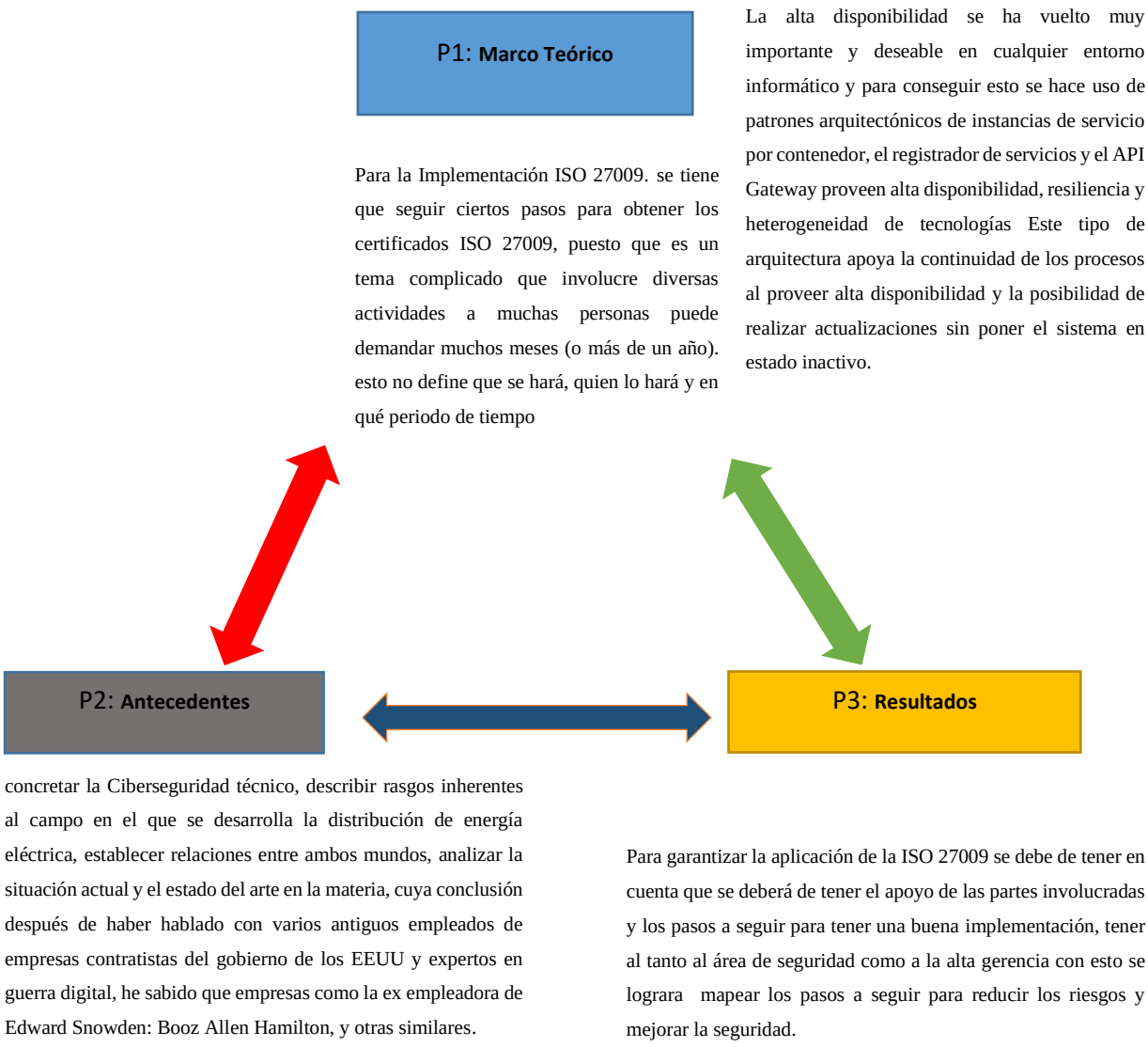

Figura 2: Triangulación de antecedentes, marco teórico y los resultados.

De acuerdo con lo expuesto se puede concluir que se deben de seguir los pasos necesarios para la aplicación de la ISO 27009 para la mejora de la seguridad de la información es necesario tener en cuenta que se reducirán los riesgos informáticos y se mejorar la seguridad de la información, se obtendrá documentación más robusta y con mejor detalle de las vulnerabilidades, esto se reflejará con la reducción de la interrupción de los usuarios.

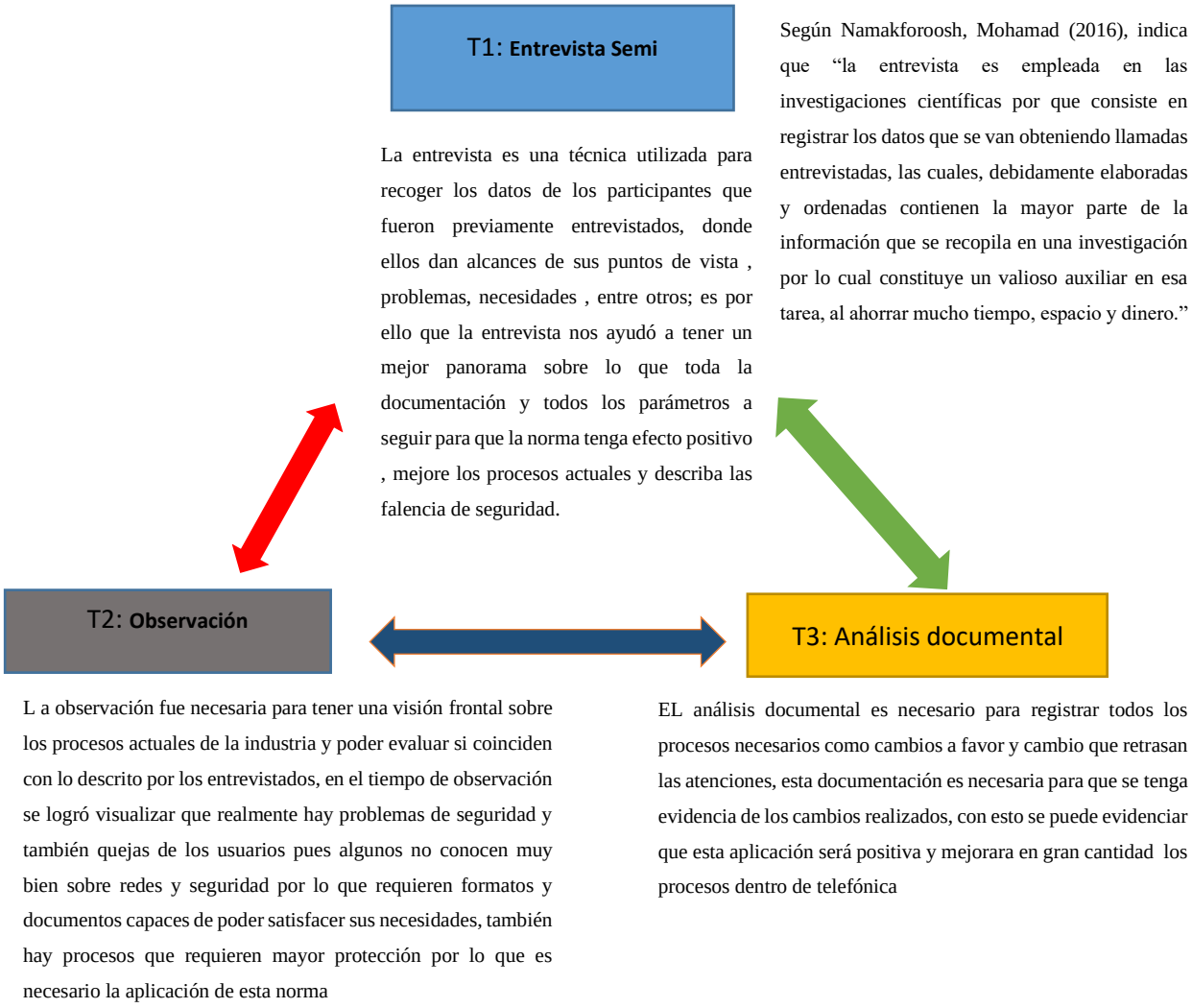

Figura 3: Triangulación de las técnicas de investigación utilizadas.

De acuerdo con lo expuesto se puede concluir lo necesario que resulta una implementación de la norma ISO 27009 que controle la seguridad. Es importante indicar que la aplicación ISO 27009 disminuirá estos posibles problemas de seguridad y agilizará sus procesos.

P1, ¿Cómo aplicar la norma ISO 27009 para prevenir riesgos del sistema de información en una empresa de telecomunicaciones?

Para la aplicación de la norma se debe diagnosticar la seguridad actual, para tener en cuenta que protocolos de seguridad se están ejecutando, para la implementación se debe tener en cuenta el inventario de activos lógicos y físicos, se deben documentar todos los procesos para tener evidencia de que se puede aumentar o que se debe quitar de la implementación,

por último, se debe monitorear y controlar las vulnerabilidades con esto evitaremos la instrucción de personas ajenas a la compañía.

P2. ¿Cómo elaborar el diagnostico de una empresa de telecomunicaciones para aplicar la norma ISO 27009?

Para el diagnostico eficiente de una empresa se debe identificar la seguridad actual para no tener redundancia en el desarrollo, luego evaluar todos los procesos de seguridad para discernir que proceso ya no es necesario y cuales deben de integrarse , el personal responsable debe haber tenido experiencia previa o capacitación del personal competente, la infraestructura lógica y física debe contar con soporte continuo para revisar las vulnerabilidades, también se deben de implementar políticas de seguridad con el fin de reducir riesgos.

P3. ¿Cómo implementar la norma ISO 27009 en una empresa de telecomunicaciones?

Para la implementación se debe tener un plan de riesgos, para evaluar los posibles riesgos, luego de este plan, se procede a la implementación siguiendo las normas y las directrices de la ISO, en este punto es importante tener planificado todos los procesos para poder diseñar un plan de mejora y volviendo más robusta la seguridad de la información.

P4. ¿Qué riesgos existe al implementar la norma ISO 27009 en una empresa de telecomunicaciones?

Es importante evaluar los riesgos de seguridad antes de la implementación de la norma una vez que se tiene los riesgos potenciales se puede ejecutar un plan de contingencia, para los riesgos encontrados para obtener una mejora continua y dar seguridad al personal que está implementando la norma.

P5. ¿Qué documentos y formatos se usan para implementar la norma ISO 27009?

Primero se diseñará los formatos, para ello se debe usar los formatos estándar establecidos en la norma para recoger todo antecedente que nos ayudara a mejorar la seguridad con ello discerniremos los métodos de información a realizar.

P6. ¿Cuáles son las estrategias del seguimiento y control?

Para el seguimiento y control es necesario realizar auditorías, ya sea interna o externas para poder visualizar que problemas se está teniendo para poder corregirlas y posterior a eso prevenir posibles vulnerabilidades.

IV. DISCUSIÓN

Para el desarrollo de la presente investigación se realizó una comparación de cada uno de los resultados obtenidos, los mismos que fueron contrastados con la documentación consultada como tesis, artículos indexados, trabajos previos, relacionándolos con cada uno de los objetivos planteados. En ese sentido el objetivo principal de esta investigación fue la implementación de la norma ISO 27009

De acuerdo a lo concluido por los tres expertos entrevistados ¿Cómo aplicar la norma ISO 27009 para prevenir riesgos del sistema de información en una empresa de telecomunicaciones?, Para que la alta gerencia se involucre con un compromiso, la norma exige como requisito técnico y financieros necesarios para que el proyecto sea terminado. dicho ambiente presenta muchos riesgos de seguridad, ofreciendo un cambio donde las amenazas son demasiadas, los déficits de seguridad son descubiertos y los incidentes se presentan con repercusiones. Para la aplicación de cualquier tipo de ISO es necesario recoger la información sobre que tipo de seguridad se está utilizando, para poder implementar un perímetro de seguridad en la que podamos registrar cuales son las vulnerabilidades actuales, para poder clasificarlas según el impacto que pueden haber dentro de la empresa en concordancia con Noguera (2019). El plan incluyo la asignación de responsabilidades, cronograma de actividades y tiempos límite para el cumplimiento de los objetivos, también hacer un listado de los procesos de información , evaluar la infraestructura (Software y hardware) con esto lograremos detectar si hay alguna interface abierta o que tan vulnerable podría ser el software por ello es necesario tener los sistemas actualizados y establecer políticas de seguridad, capaces de poder limitar a algún intruso en concordancia con Ortelli (2018) .

La Implementación de la norma ISO tuvo en cuenta el tiempo, la planeación y organización del proyecto, representando un gran esfuerzo, por lo que influye en gran medida el uso de recursos, expidiendo el proceso y niveles de gozo, de empleados en concordancia con Heffel (2016), El plan de riesgos se realizó en coordinación del equipo de TDP para que a la hora de tomar una decisión que involucre la confidencialidad o genere un grado de riesgo capaz de comprometer a la empresa en concordancia con Peña (2016). La Ejecucion del plan se debe realizar de forma progresiva, para no perturbar la atención, es necesario comunicar a las áreas involucradas, con esta medida evitaremos malos entendidos

con las distintas áreas, de esta forma se planifico cada proceso, incomodando en menos medida a los miembros de TDP en concordancia con Rocha (2019).

Según como se presentaron los riesgos se fue modelando un plan de mejora, para contrarrestar cada riesgo, mediante exhaustivos análisis y evaluando el uso diario de los miembros de TDP ,mitigando riesgos críticos y generando mayor estabilidad en el servicio en concordancia con Rodríguez (2019) .Es necesario que la Alta dirección se comprometa para el desarrollo de esta aplicación, Hay un cambio continuo en el ambiente de seguridad que presentan riesgos, siendo las amenazas y las vulnerabilidades continuas es por ellos que se realizó la documentación y la creación de formatos, estos documentos fueron realizados según fueron requeridos por los distintos departamentos en concordancia con Banda (2019).

Se diseño formatos que exige la norma en los que se tiene una mejor explicación de los procesos que se realizaron, también la creación de manuales, fueron más robustos , cualquier cambio se documenta y se guarda con un numero de requerimiento especifico, los usuarios tienen mayor conocimiento sobre los procesos y los servicios que se brindan, es por ello que se requirió una estandarización de esta documentación ,alineada a las directrices de la norma también se tendrá en cuenta el método de información, se logro tener un mejor entendimiento esto indica que los riesgos de seguridad nos ofrecen cambios continuos, las vulnerabilidades son descubiertas por lo que es necesario tener documentado el estado de seguridad actual un aspecto clave es evaluar los procesos y de esta forma los usuario tienen mayor confianza en concordancia con García (2018),.

Para realizar un buen seguimiento y control se deberá realizar algunos pasos como la identificación de la seguridad que se maneja posterior a la aplicación de la norma en la empresa, la protección de la privacidad digital, para evitar el acceso no autorizado. Se estudia los procesos de información necesario para que se cumpla los requisitos de la ISO. Los expertos son capaces de construir redes más fuertes y menos vulnerables, Las infraestructuras son más fuertes en la nube. Los acceso físico no autorizado al datacenter son restringidos mediante pases de autorización, según la jefatura que pertenezca, los firewalls son los peores centros de intuición, ya que por seguridad la última regla esta creada como un any a any(todos a todos) hacia todos los puerto con un acceso de tipo drop (Bloqueo) para restringir a las personas que intentan conectarse desde afuera. El diagnóstico de la seguridad de la información propuso un enfoque sistémico y por objetivos, aplicado a los principios básicos del diagnóstico con la definición de los objetivos, la identificación de activos y

recursos así mismo, de cada una de ellas deben verificarse diferentes aspectos básicos relacionados con la normativa vigente, la aplicabilidad al caso real de la organización, la eficiencia del control ejercido la empleabilidad y la formación del personal encargado también el diagnóstico del Hardware, Software. la revisión preliminar de los sistemas de información, realizada por medio del internet y los conocimientos adquiridos del equipo de trabajo ayudara a recolectar información sobre la infraestructura de los equipos intermediarios sin embargo las políticas de seguridad actuales comprender el diagnóstico de sistemas de información y la propuesta de plataforma de información en concordancia con Yañez (2018).

La norma ISO 27009 brinda parámetros de seguridad, capaces de cerrar puertas traseras, para evitar que se infiltre personas ajenas al servicio, mediante políticas de seguridad mas restrictivas estos reglamentos son denominados como controladores de seguridad, ya que indican los pasos a seguir para tener una secuencia de seguridad informática, para la aplicación de la norma ISO 27009 es necesario evaluar cuales son los riesgos, y que debemos de mejorar para que los colaboradores y los clientes cuenten con un grado de confianza para solicitar el servicio, es necesario realizar auditorías internas o externas, estas auditorias someterán al sistema de información ,con eso se lograr deslumbrar los riesgos de información, es usual realizar este tipo de auditorías, pues ayudaron al sistema para estar preparado ante algún ataque informático Olivares (2016) .

Las acciones correctivas se efectuaron después de haber detectado las vulnerabilidades, estas acciones se realizaron luego de las auditorias esta acción fueron requeridos para evitar los riesgos potenciales dentro de la industria, también se realizó las acciones preventivas estas medidas se usan como contingencia para que se logre tener un accionar más rápido y restringir a los intrusos mediante estas medias .Por tanto para la mejora de los procesos de seguridad, tanto como denegación de servicios a intrusos o restricción de permisos a personal no autorizado es necesario esta norma ya que indica los distintos puntos de vista para mejorar la seguridad de la información, obtuvo mayor confianza para ejecutar aplicaciones específica, también mejorar la documentación de los distintos procesos ya sea con informes gerenciales o distintos documentos necesarios para la seguridad ;también reducido la interrupción del personal inexperto de la seguridad de la información y tendrán un mejor perfil para el desarrollo de los distintos proyectos que tengan en mente ejecutar o que estén en proceso de desarrollo Rodríguez (2016).

V. CONCLUSIONES

Primera

Para la aplicación de la norma ISO 27009 se concluyó que se determinó la influencia de la aplicación de la norma para prevenir los riesgos del sistema de información esto aumento la seguridad y la confianza de los colaboradores para poder trabajar de una forma mas eficiente y segura.

Segunda

Para la aplicación de la norma ISO 27009 se concluyó que se determinó la disponibilidad de la aplicación de la norma para prevenir los riesgos del sistema de información esto aumento el tiempo de reacción ante un ataque informático, creando parámetros de contingencia capaces de responder, ante alguna incidencia.

Tercera

Para la aplicación de la norma ISO 27009 se concluyó que se determinó la confidencialidad de la aplicación de la norma para prevenir los riesgos del sistema de información esto aumento la seguridad para mantener los datos personales de cada usuario, evitando vulnerar la información privada, para evitar la suplantación de usuario, logrando evitar el difundir información confidencial,

Cuarta

La aplicación de la norma ISO 27009 tuvo como conclusión una mejor documentación, de contenido más descriptivo y mejor entendimiento por los miembros de las distintas áreas, también esta documentación fue capaz de reducir el tiempo de interrupción generando tiempo más productivo para realizar otras funciones.

Quinto

La aplicación de la norma ISO 27009 tuvo como conclusión tener auditorias más descriptivas para poder evaluar los riesgos encontrados y poder crear un perímetro de seguridad, capaz de restringir a los intrusos, este tipo de análisis ayudo a verificar que tan seguro es nuestro sistema de seguridad.

VI. RECOMENDACIONES

Primera

Se recomienda al jefe de seguridad de TDP que se debe determinar la influencia de la aplicación de la norma periódicamente, ya que permite detectar puertas traseras e identificar, las vulnerabilidades una norma de otra para posteriormente migrar a una mas reciente, para obtener mejor seguridad.

Segunda

Se recomienda al gerente de seguridad de TDP que se determine la disponibilidad de la aplicación constantemente mediante un script (Secuencia de comandos) de alertas indicando que dejo de funcionar tal equipo, ya que el modo grafico tiene un retardo de 30 minutos, generando quejas por los miembros de distintas áreas al momento de caer un servicio.

Tercera

Se recomienda al usuario evitar compartir las contraseñas estáticas, ya que algún usuario malicioso podría manipular su computadora remotamente y vulnerar esta puerta trasera causando falta de confidencialidad y suplantación de usuario.

Cuarta

Se recomienda al supervisor de seguridad de TDP revisar la documentación que este alineada a las directrices de la norma, para tener documentos y formatos con información mas descriptiva, estos formatos serán mas entendible para los nuevos usuarios que se integren al equipo de trabajo.

Quinto

Se recomienda al jefe de seguridad de TDP realizar auditorias trimestrales , para poder detectar vulnerabilidades que se encuentran dentro y fuera de la empresa, para evitar los riesgos de ataques informáticos.

REFERENCIAS

Abanto, J. & Asensio, S. (2017). Centro de Ciberseguridad Industrial. Estudio sobre el estado de la Ciberseguridad Industrial en Perú. ISACA. Recuperado de: https://www.cci-es.org/web/cci/detalle-actividad/-/journal_content/56/10694/452983;jsessionid=26CDA3DBD58CAAC3FDA5B73BD2D9359C

Acosta, J. (2017). El camino hacia la resiliencia cibernética. Encuesta Global de Seguridad de la información 2016-17. Recuperado de http://www.ey.com/Publication/vwLUAssets/EY-el-camino-hacia-resilienciacibernetica/$FILE/EY-el-camino-hacia-resiliencia-cibernetica.pdf

Alcalde (2016).Seguridad de la información amenazas y desafios.Recuperado en: http://www.ceptm.iue.edu.ar/pdf/seguridadDeLaInformacion.pdf

Álvarez. Asistente para la Realización de Auditorías de Sistemas en Organismos Públicos o Privados. 2015. Recuperado de: http://laboratorios.fi.uba.ar/lsi/rgm/tesistas/kuna-tesisdemagister.pdf

Ayala, M. (2017). Sistema de gestión de seguridad de información Para mejorar el proceso de gestión del riesgo En un hospital nacional, 2017. Tesis, Universidad César Vallejo, Lima Perú. Recuperado de: http://repositorio.ucv.edu.pe/bitstream/handle/UCV/13753/Ayala_MMA.pdf?sequence=1&isAllowed=y

Banda, D. y Rodríguez, J. Metodologías de gestión de riesgos de ti para contribuir en la mejora de la seguridad de los activos de información en empresas del sector agroindustrial de la región lambayeque. Recuperado de: http://blogs.unellez.edu.ve/dsilva/files/2014/07/Metodologia-XP.pdf

Bernaldo, N. (2016). Sistema de gestión de seguridad de la Información en el Proceso de Registros Civiles de RENIEC. San Borja. Lima 2016. Tesis, Universidad César Vallejo, Lima. Recuperado de: http://repositorio.ucv.edu.pe/bitstream/handle/UPN/18753/Bernaldo_MMA.pdf?sequence=1&isAllowed=y

Betacourt A. (2018). Metodología de correlación estadística de un sistema integrado de gestión de la calidad en el sector salud. Revista Signos, 10 (1), 10. Recuperado de: http://revistas.usantotomas.edu.co/index.php/signos/rt/printerFriendly/4681/html

Celí. E. (2016). La gestión de riesgo TI y la efectividad de los sistemas de seguridad de información: caso de procesos críticos en las pequeñas entidades financieras de Lambayeque. Pueblo Cont. 27(1). 73-84. Recuperado de: http://journal.upao.edu.pe/PuebloContinente/article/download/395/360 40

Centro Criptológico Nacional (2018) Ciberamenazas y Tendencias Edición. Recuperado de: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2835-ccncert-ia-09-18-ciberamenzas-y-tendencias-edicion-2018-1/file.html

Chugcho, M.(2018) .La gestión de Producción y su relación con la optimización de recursos materiales en la empresa Karitex del Cantón Pelileo. Recuperado en : https://repositorio.uta.edu.ec/handle/123456789/8235

Class & Asociados S.A (2018). Informe de clasificación de riesgo Mapfre Perú Vida Compañía de Seguros y Reaseguros. Recuperado de: http://www.smv.gob.pe/ConsultasP8/temp/MPV311217.pdf

De La cruz, R. (2016). Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la municipalidad provincial de Paita; 2016. Tesis, Universidad Católica Los Ángeles Chimbote, Piura. Recuperado de: http://repositorio.uladech.edu.pe/handle/123456789/885

Díaz, R. (2015). Apoyo al proceso de implementación de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001:2013 en la alcaldía de Pasto. Tesis, Universidad de Nariño, Colombia. 86. Recuperado de: http://biblioteca.udenar.edu.co:8085/atenea/biblioteca/91046.pdf

Duque, A. C. (2017). Methodology for risk management. How to integrate security into strategic business objectives in a cost-effective way. Retrieved abril 10, 2017, 41.Recuperado de: http://www.ridsso.com/documents/ muro/207_1469148692_57916e1488c74.pdf

Frascati, M. (2020). Propuesta de Norma Práctica para Encuestas de Investigación y Desarrollo Experimental. Recuperado de: http://www.idi.mineco.gob.es/stfls/MICINN/Investigacion/FICHEROS/ManuaFrascati-2002_sp.pdf ISBN: 84-688-2888-2

Garcia, D. (2015). Ciberseguridad: qué es y para qué sirve. Obtenido de https://www.ucavila.es/blog/2015/07/03/ciberseguridad-que-es-y-para-que-sirve/ 86

García (2018). Modelo de seguridad de la información para el apoyo en la gestión ambiental en Lambayeque. Recuperado en: http://hdl.handle.net/20.500.12423/1488

Gestión. (2017). Perú registrará US$ 4,782 millones en pérdidas por ciberdelitos en 2017. Recuperado de https://gestion.pe/tecnologia/peru-registraraus-4-782-millones-perdidas-ciberdelitos-2017-141411

Gómez(2017). Técnicas e instrumentos de recolección de datos para investigaciones Científicas.Recuperado en: http://www. ciencias.edu.pe/pdf/documentos- educacion-academicos/de-la-postgradoune /23.pdf

Gómez(2017).Sistema de informacion en ciencias de la computación.Recuperado en: https://dspace.ups.edu.ec/bitstream/123456789/14907/1/Sistemas%20de%20informacion%20en%20ciencias%20de%20la%20computacion.pdf

Guárdia, Joan. 2018. Análisis de datos en psicología [en línea]. 2a ed. Madrid: Delta Publicaciones. Recuperado de: https://books.google.com.pe/books?id=KnvzOlV_k9IC&pg=PA193&dq=coeficiente+de+correlacion+de+pearson&hl=es-419&sa=X&ved=0ahUKEwj6

Guillermo, Néstor. 2016. Estudio de prefactibilidad para la creación de una empresa dedicada a la industrialización y comercialización de los derivados de la caña de azúcar. Lima: PUCP. Recuperado de: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/4994/GUILLERMO

Heffel (2016) Ciberseguridad industrial en la distribución de energía eléctrica recuperado en : http://mendillo.info/seguridad/tesis/Heffel.pdf

Heradia,(2018). Sistema de indicadores para la mejora y el control integrado de la calidad de los procesos. España: Universidad Jaume I. Disponible en: https://books.google.com.pe/books?id=uLIt7WeQ7N4C&pg=PA28&dq=eficacia+en+una+empresa+de+servicio&hl=es&sa=X&ved=0ahUKEwi6g_

Hernández , Fernández y Baptista.Método y metodología en la investigación bj.Recuperado en: https://es.slideshare.net/digraficaimprentaeditorial/mtodo-y-metodologa-en-la-investigacin-bj

Hinojosa, M. (2015). la implementación de un SGSI.Recuperado en: https://reunir.unir.net/bitstream/handle/123456789/3129/HelenaClaraIsabel_Aleman_Novoa.pdf?sequence=1&isAllowed=y

Humphreys (2017). Llevando la gestión de la seguridad de la información a otro nivel con una nueva norma para sectores específicos del mercado.Recuperado de : https://www.dnvgl.es/news/llevando-la-gestion-de-la-seguridad-de-la-informacion-a-otro-nivel-con-una-nueva-norma-para-sectores-especificos-del-mercado-79375

ISO. (2018). ISO/IEC 27002:2018. Information technology — Security techniques — Code of practice for information security controls. Revisión marzo 17, 2015, Recuperado de: http://www.iso.org/iso/catalogue_detail?csnumber=54533 42

ISO. (2017). ISO Survey 2015. Retrieved March 15, 2017, Recuperado de: https://www.iso.org/ the-iso-survey.html

Jiménez, Vicente, E., & Mateos, A. (2015). Selection of safeguards in risk management in information systems: a blurred approach. RISTI - Magazine System and Technology Information, (15), 83–100. http:// doi.org/10.17013/risti.15.83-100

ISO/IEC 27000. (2016). Information technology — Security techniques — Information security management systems — Overview and vocabulary. Suiza: ISO copyright office.

Kosutic (2019). ISO/IEC 27009:2016 Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements.Recuperado en: https://www.iso.org/standard/42508.html

Mercado, J.(2016). gestión de seguridad de la información para el E-Gobierno Recuperado de https://books.google.com.pe/books?id=-XG4KMFNnP4C&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepag&q&f=false

Morales, M.(2017). Metodología de la Investigación. Recuperado en: https://www.academia.edu/20792455/Metodolog%C3%ADa_de_la_Investigaci%C3%B3n_5ta_edici%C3%B3n_-_Roberto_Hern%C3%A1ndez_Sampieri

Moscoso L, Esau E y Soto C (2018). Modelo de gestión de riesgos de TI que contribuye a la operación de los procesos de gestión comercial de las empresas del sector de 43 saneamiento del norte del Perú. Recuperado de: http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.6EDBFCEC&lang=es&site=eds-live

Nazareno(2017). Auditoría informática en el área administrativa de la pontificia universidad católica del ecuador sede esmeraldas. Tesis de grado. Pontificia Universidad Católica

de Ecuador.Recuperado en: http://repositorio.ucv.edu.pe/Nzareno_MMA.pdf?/handle/UCV/13753/sequence=1&isAllowed=ybitstream

Noguera A. (2019). Aplicación de un sistema para detectar intrusos para la empresa Venezolana del vidrio S.A , resuprado de:http://mendillo.info/seguridad/tesis/Noguera.pdf

Olivares (2016). modelo de la gestion de la seguridad en la información para el e-gobierno.Recuperado en https://dialnet.unirioja.es/descarga/articulo/5858354.pdf

Ortega, M. (2016). El recurso de la metodología. Camino a la investigación.Recuperado en :https://www.researchgate.net/publication/263280163_El_Recurso_de_la_metodologia_Camino_a_la_Investigacion

Ortelli (2018) . Normativa aplicada en la seguridad informática tuvo como objetivo investigar la gerencia y la problemática que conllevó al tema de la seguridad informática en las diversas organizaciones modernas (Caso de Gandalf Comunicaciones, C.A.) .Recuperado de : http://www.experimental.edu.pe/documentos/.postgradoune.pdf

Peña (2016).Diseño e implementación de una red privada virtual (VPN-SSL) utilizando el método de autenticación ldap en una empresa privada. recuperado en :http://mendillo.info/seguridad/tesis/Pe%C3%B1a.pdf

Rivero, P. (2017). Diseño de un modelo de gestión del riesgo aplicado a una empresa manufacturera de autopartes. Tesis, Instituto Politécnico Nacional, México. 44 recuperado en: http://vitela.javerianacali.edu.co/bitstream/handle/11522/11277/Dise%C3%B1o_sistema_Gestión.pdf?sequence=1&isAllowed=y

Rocha (2019). Modelo de gestión de seguridad informática para el sector público.Recuperado en : http://157.100.241.244/bitstream/47000/1863/1/UISRAEL-EC-MASTER%20-%20TELEM-378.242-2019-001.pdf

Rodríguez, (2019). Gestión de riesgos de tecnologías de la información como apoyo en la continuidad del negocio en una empresa que brinda software. España. http://es.scribd.com/doc/31440864/Metodologia-RUP

Rodríguez (2016). factores que dañan la implementación de un SGSI en entidades públicas peruanas en referencia de la NTP - ISO/IEC 27009.Recuperado en: https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/4884/Seclen_aj.pdf?sequence=1&isAllowed=y

Rodríguez. (2016). Diseño y formulación de un sistema de gestión de riesgos basados en los lineamientos establecidos por la norma NTC- ISO 31000 versión 2011 para la empresa Simma Ltda. Tesis, Universidad Industrial de Santander, Colombia. Recuperado de: http://tangara.uis.edu.co/biblioweb/tesis/2016/163435.pdf

SGSI. (2015). ISO 27001: Amenazas y vulnerabilidades. Obtenido de http://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/

Tarrillo, E. (2016). Influencia de la Gestión de Riesgo en la seguridad de Activos de Información de la zona Registral III Sede Moyobamba, 2015. Tesis, Universidad César Vallejo, Tarapoto. Recuperado de: http://repositorio.ucv.edu.pe/handle/UCV/1286

Telefónica del Perú. (2017). Certificados y normas ISO para sus servicios. Recuperado de:http://www.postgradoune.edu.pe/documentos/Experimental.pdf

Valencia, H. (2016). Metodología del SGSI Según La Norma ISO/IEC 27001 para el gobierno autónomo descentralizado de San Miguel de Urcuquí. Tesis, Universidad Técnica Del Norte, Ibarra- Ecuador. Recuperado de: http://repositorio.utn.edu.ec/handle/123456789/5714

Velásquez P, Velásquez S, Velásquez M y Villa J (2017). Implementación de la gestión de riesgo en los procesos misionales de la Sección de Dermatología de la Universidad de Antioquia (Medellín, Colombia) siguiendo las directrices de la norma ISO 9001:2015. Revista Gerencia y Políticas de Salud, 16(33), 78–101. http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=1&sid=4c561103-d180-4b5f-9baa-4c12a14e149d%40sessionmgr4008

Yañez, D. (2018). sistema de gestión de seguridad de la información para la subsecretaria de economía y empresas de menor tamaño. Recuperado de http://repositorio.uchile.cl/bitstream/handle/2250/147976/Sistema-de-gestion-de-seguridad-de-la-informacion-para-la-Subsecretaria-de-Economia-y-Empresas.pdf?sequence=1&isAllowed=y

ANEXOS

Anexo 1: Matriz de categorización

Titulo: Aplicación de la norma ISO 27009 para prevenir riesgos del sistema de información en la empresa Telefónica, Surquillo
Nombres: Luigi Chipulina Puelles

Problema general	Objetivo general	Categorías	Sub categorías	Técnicas	instrumento
¿De qué manera influye una Aplicación de la norma ISO 27009 para prevenir riesgos del sistema de información en la empresa Telefónica, Surquillo **Problema Especifico 1:** ¿En qué medida una aplicación de la Norma IS0 27009 influye en la disponibilidad de la seguridad de la información? **Problema Especifico 2** ¿En qué medida una aplicación de la Norma IS0 27009 influye en la confidencialidad de la seguridad de la información?	Determinar la influencia de una aplicación de la norma ISO 27009 para prevenir los riesgos del sistema de información en la empresa Telefónica, Surquillo **Objetivo Específico 1 :** Determinar la influencia de una aplicación de la norma ISO 27009 en la disponibilidad del sistema de información en la empresa Telefónica, Surquillo **Objetivo Especifico 2:** Determinar la influencia de una aplicación de la norma ISO 27009 en la confidencialidad del sistema de información en la empresa Telefónica, Surquillo	Diagnostico Implementación de la norma Documentación y formatos Seguimiento y control	• Identificación de seguridad • Proceso de información • Competencia del personal • Infraestructura • Políticas de seguridad • Plan de riesgos • Ejecución del plan • Planificación de los procesos • Plan de mejora • Diseño de formatos • Estandarización de la Información • Método de información • Auditorías • Acciones correctivas • Acciones Preventivas	Entrevistas Observación Análisis documental	Guía de entrevistas Guías de observación Ficha de análisis documental

Fuente: Sampieri (2019)

Anexo 2: Instrumentos de recolección de datos

Guía de Entrevista

"Aplicación de la norma ISO 27009 para prevenir riesgos del sistema de información en la empresa Telefónica, Surquillo"

1, ¿Cómo aplicar la norma ISO 27009 para prevenir riesgos del sistema de información en una empresa de telecomunicaciones?

2. ¿Cómo elaborar el diagnostico de una empresa de telecomunicaciones para aplicar la norma ISO 27009?

a) ¿Cómo identificar los posibles riesgos de seguridad?
b) ¿Cómo identificar los procesos de información de seguridad?
c) ¿Cómo determinar la competencia del personal para aplicar la norma ISO 27009?
d) ¿Cómo determinar la infraestructura del proceso de seguridad de la Información?
e) ¿Cómo identificar las políticas de seguridad?

3. ¿Cómo implementar la norma ISO 27009 en una empresa de telecomunicaciones?

4. ¿Qué riesgos existe al implementar la norma ISO 27009 en una empresa de telecomunicaciones?

a) ¿Cómo se realizaría un plan riesgos?
b) ¿En qué consiste la ejecución del plan de riesgos?
c) ¿Cómo planificar los procesos de ejecución de la norma ISO 27009?
d) ¿Cómo se realizaría un plan de mejora?

5. ¿Qué documentos y formatos se usan para implementar la norma ISO 27009?

a) ¿Qué formatos son los necesarios a diseñar para implementar la Norma ISO 27009?
b) ¿Cómo ejecutar la estandarización de la norma ISO 27009?

c) ¿Qué métodos de información son los más comunes usando la Norma ISO 27009?

6. ¿Cuáles son las estrategias del seguimiento y control?

a) ¿Qué tipo de auditorías hay que hacer?
b) ¿Cómo se determinan las acciones correctivas?
c) ¿Cómo se determinan las acciones preventivas?

Anexo 3: Matriz de desgravación de entrevista

N°	PREGUNTAS	Entrevista 1: Jefe de Seguridad de TDP
1	¿Cómo aplicar la norma ISO 27009 para prevenir riesgos del sistema de información en una empresa de telecomunicaciones?	El compromiso de la alta dirección es necesario no solo porque la norma lo exige como requisito, sino porque de esto dependen todos los recursos humanos, técnicos y financieros necesarios para llevar el proyecto hasta su culminación. El ambiente dinámico que presentan los riesgos de seguridad nos ofrece cambios continuos, donde las amenazas son constantes, las vulnerabilidades son descubiertas y los incidentes de seguridad se presentan con repercusiones importantes, ya sea para las organizaciones o para las personas. Para aplicar la norma ISO se debe saber desde qué punto partimos para la certificación es imprescindible elaborar un diagnóstico de la situación actual de la empresa, esta información base es relevante para analizar la viabilidad de cumplimentación de los requisitos necesarios para implementar las normas ISO que se quieran certificar, una vez que la empresa ha evaluado su situación inicial, deberá abordar un plan de implantación documentado. Este plan exige la identificación y descripción de procesos necesarios para que el sistema cumpla con todos los requisitos del estándar ISO, El plan deberá incluir la asignación de responsabilidades, cronograma de actividades y tiempos límite para el cumplimiento de los objetivos (Seguimiento y control).
2	¿Cómo elaborar el diagnostico de una empresa de telecomunicaciones para aplicar la norma ISO 27009?	Para un correcto diagnostico hay una serie de pasos que debemos que tener en cuenta, primero habrá que Identificar la seguridad de la información actual como las medidas de protección de la privacidad digital que se aplican para evitar el acceso no autorizado a los datos, luego se evalúan los procesos de la información necesarios para que el sistema cumpla con todos los requisitos del estándar ISO , todo esto ha impulsado una demanda de soluciones y expertos en seguridad de datos que sean capaces de construir redes más fuertes y menos vulnerables. La idea de que las infraestructuras locales son más seguras que las infraestructuras en la nube es un mito. El acceso físico no autorizado a los centros de datos en la nube es extremadamente raro. Las peores infracciones ocurren detrás de los firewalls de las empresas y de sus propios empleados. Los datos en una nube pueden residir en cualquier número de servidores en cualquier número de ubicaciones, en lugar de un servidor dedicado dentro de la red local. el cumplimiento de las políticas y leyes de privacidad, y las organizaciones deben supervisar cualquier actividad sospechosa, el acceso a datos no autorizados y remediar con controles de seguridad, alertas o notificaciones a todo aquello que las entidades consideran importante o de alta validez para la misma, ya que puede contener información importante como lo puede ser bases de datos con usuarios, contraseñas, números de cuentas, etc.
3	¿Cómo implementar la norma ISO 27009 en una empresa de telecomunicaciones?	Para la implementación de la norma deberíamos tener en cuenta las vulnerabilidades antes de diseñar un plan para solucionar las pruebas de intrusión que implican la ejecución del plan de procesos manuales o automatizados que interrumpen los servidores, las aplicaciones, las redes e incluso los dispositivos de los usuarios finales para ver si la intrusión es posible y dónde se produjo esa ruptura, para la planificación de los procesos se realiza mediante una secuencia ordenada de pasos, estos procesos de administración están diseñados para la seguridad de datos y finalmente el Plan de mejora nos permite elaborar un plan de contingencia para atacar los riesgos que aparezcan en el Proyecto y corregirlo al momento .
4	¿Qué riesgos existe al implementar la norma ISO 27009 en una empresa de telecomunicaciones?	Los negocios comparten una serie de riesgos comunes y contienen otros específicos de su organización. Existen algunas guías o listas que nos pueden ayudar a verificar si esos riesgos comunes que comparten la mayoría de las organizaciones nos afecta en la seguridad de la información también es necesario elaborar un plan de riesgo para tener en cuenta los métodos sofisticados para neutralizar a los intrusos porque para la ejecución del plan de riesgo se debe tener claro todas los accesos

		denegados para estos delitos, es por ello que se realizara una planificaremos de los procesos con ello tendremos una relación de riesgos , por lo que el plan de mejora nos ayudara para subsanar aquellos vacíos de seguridad por lo que se mejorara la eficiencia y eficacia
5	¿Qué documentos y formatos se usan para implementar la norma ISO 27009?	El Diseño de formatos exige la identificación y descripción de procesos necesarios para que el sistema cumpla con todos los requisitos del estándar ISO, deberá incluir la asignación de responsabilidades, cronograma de actividades y tiempos límite para el cumplimiento de los objetivos ,una vez que se genera la documentación necesaria, es preciso crear un método que permita el control de los documentos, siendo un medio para gestionar la creación, aprobación, distribución, revisión, almacenamiento, modificación y eliminación de los diferentes documentos que se tramiten en la empresa.
6	¿Cuáles son las estrategias del seguimiento y control?	El procedimiento de Seguimiento y Control del Proyecto establece el conjunto de acciones que se llevarán a cabo para la comprobación de la correcta ejecución de las actividades del proyecto, por lo que urge conocer la eficiencia del sistema y conocer los posibles fallos que pueden presentarse. La mejor forma de hacerlo es mediante la realización de una auditoría interna es preciso que la alta dirección haga una revisión de la labor general y verifique el cumplimiento de las acciones correctivas determinadas durante la auditoría interna luego de observar estas observaciones por parte de las auditorias realizaremos acciones Preventivas para evitar vulnerabilidades y restringir a los intrusos

N°	PREGUNTAS	Entrevista 2: Gerente de Seguridad de TDP
1	¿Cómo aplicar la norma ISO 27009 para prevenir riesgos del sistema de información en una empresa de telecomunicaciones?	Para aplicar la norma se debe planificar bien y con tiempo, la planeación y la organización del proyecto representan un gran esfuerzo, por lo que influye en gran medida sobre el uso de recursos, lo expedito del proceso y el nivel de satisfacción de los empleados para el diagnóstico de la seguridad de la información debemos tener en cuenta que al investigar y analizar los riesgos asociados a los procesos del propio negocio y su entorno, una de las primeras actividades a realizar en la implementación de la norma en una empresa de telecomunicaciones es elaborar un inventario de activos que recoja cuáles son los principales activos de información en la organización, para establecer un expediente de registro de evidencias, organice la documentación solicitada, recopile actas y material relacionados con las pruebas realizadas o elaboración de formatos necesarios usar procedimientos en condiciones reales de operación para validar el diseño, la documentación e implementación del sistema de calidad.
2	¿Cómo elaborar el diagnostico de una empresa de telecomunicaciones para aplicar la norma ISO 27009?	El diagnóstico de la seguridad de la información propone un enfoque sistémico y por objetivos, aplicado a los principios básicos de evidencia, análisis, síntesis y de control ,el procedimiento para el diagnóstico se puede resumir de la siguiente forma, el diagnóstico con la definición de los objetivos, la identificación de activos y recursos, seguidamente se aplica las técnicas para evaluar los recursos disponibles, aplicando el enfoque a procesos de información para evaluar globalmente todas las áreas de la organización ,así mismo, de cada una de ellas deben verificarse diferentes aspectos básicos relacionados con la normativa vigente, la aplicabilidad al caso real de la organización, la eficiencia del control ejercido, el valor económico, la empleabilidad y la formación del personal encargado también el diagnóstico del Hardware, Software y la evaluación de las políticas de seguridad.
3	¿Cómo implementar la norma ISO 27009 en una empresa de telecomunicaciones?	La organización con respecto a los niveles de madurez requeridos, evaluar los riesgos, analizar los controles y poder determinar un plan de riesgo, para comenzar a trabajar en los procesos críticos para la organización por consiguiente la ejecución del plan para implementar la norma, el equipo encargado debe tener presente los criterios de medición y objetivos comprobados(Planificación de los procesos) ,también será necesario una serie de recomendaciones para poder incorporar un plan de mejora
4	¿Qué riesgos existe al implementar la norma ISO 27009 en una empresa de telecomunicaciones?	Para evaluar los riesgos se debe analizar los controles y poder determinar un plan de riesgo, para comenzar a trabajar en la ejecución del plan de la organización, luego para la planificación de procesos se analiza el previo diagnóstico eficiente de seguridad de la información es por este motivo que se recomienda el análisis funcional de la organización, considerando un plan de mejora que e se encuentran inmersas dentro del ciclo de mejora continua PHVA (Planear, Hacer, Verificar y Actuar), y puede ajustarse y acomodarse al tipo de empresa a la cual se quiera aplicar.
5	¿Qué documentos y formatos se usan para implementar la norma ISO 27009?	La Documentación de lo que se haga proporciona visibilidad del proyecto, una guía para el trabajo, una base de referencia para revisar el avance y un registro de lo realizado como referencia futura, aunque se debe evitar documentar lo innecesario, el diseño de formatos pueden iniciar con anticipación en el proyecto y son paralelas a las etapas planes de organización y calidad estos elementos se estandarizan con su documentación formal para su posterior implementación los cambios finales a la documentación y el cierre de cualquier no conformidad en la implementación se traslapan con la validación del sistema de seguridad, la cual se debe asegurar los métodos de información para su

		participación en el análisis, redefinición y documentación de sus labores es esencial.
6	¿Cuáles son las estrategias del seguimiento y control?	Contar con un sistema de seguimiento y control que funcione, que asegure una calidad consistente del producto, con los registros adecuados para verificarlo, por lo que requiere auditorías a los procedimientos, para verificar su consistencia y compatibilidad con el resto de la documentación y a las instrucciones de trabajo con el fin de verificar su adecuación con los requisitos de la norma, los procedimientos de acción correctiva y acción preventiva , facilitan el proceso de perfeccionar, diseñar, documentar e implementar los elementos del sistema de calidad, así como para solucionar las no conformidades identificadas durante la evaluación del mismo.

N°	PREGUNTAS	Entrevista 3: Supervisor de Seguridad de TDP
1	¿Cómo aplicar la norma ISO 27009 para prevenir riesgos del sistema de información en una empresa de telecomunicaciones?	El ambiente dinámico que presentan los riesgos de seguridad nos ofrecen cambios continuos, donde las amenazas son constantes, las vulnerabilidades son descubiertas y los incidentes de seguridad se presentan con repercusiones importantes, ya sea para diagnosticar el estado en el que se encuentra, se debe revisar las falencias y revisar cual es el estado de seguridad actual para la implementaciones la normales un aspecto clave en cualquier organización que desea alinear sus objetivos y principios de seguridad de la información, también se debe documentar todos los procesos y de ser necesario diseñar formatos para que obtengamos un mejor seguimiento y control de los procesos deben incluir la verificación de las acciones llevadas acabo
2	¿Cómo elaborar el diagnostico de una empresa de telecomunicaciones para aplicar la norma ISO 27009?	Es importante mencionar que el diagnóstico y la propuesta: la revisión preliminar de los sistemas de información, realizada por medio del internet y los conocimientos adquiridos del equipo de trabajo ayudara a recolectar información sobre la infraestructura de los equipos intermediarios como firewalls , switches o sistemas de seguridad que se encuentran corriendo, sin embargo las políticas de seguridad actuales comprender el diagnóstico de sistemas de información y la propuesta de plataforma de información y comunicación son última instancia estos fueron insumos importantes y fundamentales para el desarrollo de este proyecto de investigación
3	¿Cómo implementar la norma ISO 27009 en una empresa de telecomunicaciones?	Si la empresa quiere implementar la norma ISO, puede resultar abrumador averiguar por donde comenzar por este motivo, es necesario tener un buen argumento para convencer a la dirección que implementa la norma ISO, en función del plan de riesgos y ejecución en materia de seguridad de la información que se han identificado, se desarrollan procedimientos para eliminar o, en su defecto, controlar dichos riesgos con el fin de asegurar que los procesos tengan los recursos suficientes para ser eficientes y mejorar, la dirección necesita revisar datos específicos de las actividades.
4	¿Qué riesgos existe al implementar la norma ISO 27009 en una empresa de telecomunicaciones?	Las empresas con el fin de evitar la aparición de riesgos inesperados que puedan afectar a cualquier incidencias de seguridad deberá de elaborarse un plan de riesgos principalmente porque afecta la información y los sistemas, la solución para las incidencias de seguridad son mucho más que implementar tecnología como firewalls y gateways, antivirus, es importante tener en cuenta que el propósito de los sistemas de información y los datos que contienen es apoyar los procesos de negocios, que a su vez apoyan la misión de la organización. En un sentido muy real, la información es un elemento fundamental que apoya al negocio y su misión, y contribuye a la capacidad de una organización para sostener las operaciones.
5	¿Qué documentos y formatos se usan para implementar la norma ISO 27009?	La documentación de la norma Identifica las entradas necesarias y salidas de cada uno de los procesos de la organización determinando las secuencias e interacción de todas las actividades. debe tener un diseño de formatos según la directriz de la norma y también tendrá un formato estándar para poder registrar los datos necesarios y debe ser redactado antes que se realice la evaluación y el tratamiento de riesgos y el informe de evaluación y allí se resumen todos los resultados.
6	¿Cuáles son las estrategias del seguimiento y control?	Las estrategias existen para que cada extremo presente alguna sugerencia de desarrollo del sistema de información usando un marco lógico con el plan de auditoria, se debe contar con el nivel de importancia de los procesos y de las áreas que van a ser auditadas y, además, hay que tener en cuenta los resultados obtenidos de auditorías previas también es necesario definir los criterios utilizados durante la auditoría, el alcance, la frecuencia y los métodos utilizados para las acciones correctivas la organización debe velar por mantener y mejorar su sistema de seguridad de la información para realizar el levantamiento de registros los cuales deben ser legibles, identificables y trazables se

		toman las acciones necesarias para prevenir una posible intrusión, estas acciones se pueden realizar tanto a nivel de software (actualización del sistema), a nivel hardware (p.e. asegurar físicamente nuestro servidor) o de red (filtrado de puertos).

Anexo 4: Matriz de desgravación y codificación

N°	PREGUNTAS	Entrevista 1: Jefe de Seguridad de TDP	Entrevista
1	¿Cómo aplicar la norma ISO 27009 para prevenir riesgos del sistema de información en una empresa de telecomunicaciones?	El compromiso de la alta dirección es necesario no solo porque la norma lo exige como requisito, sino porque de esto dependen todos los recursos humanos, técnicos y financieros necesarios para llevar el proyecto hasta su culminación. El ambiente dinámico que presentan los riesgos de seguridad nos ofrece cambios continuos, donde las amenazas son constantes, las vulnerabilidades son descubiertas y los incidentes de seguridad se presentan con repercusiones importantes, ya sea para las organizaciones o para las personas. Para aplicar la norma ISO se debe saber desde qué punto partimos para la certificación es imprescindible elaborar un diagnóstico de la situación actual de la empresa, esta información base es relevante para analizar la viabilidad de cumplimentación de los requisitos necesarios para implementar las normas ISO que se quieran certificar, una vez que la empresa ha evaluado su situación inicial, deberá abordar un plan de implantación documentado. Este plan exige la identificación y descripción de procesos necesarios para que el sistema cumpla con todos los requisitos del estándar ISO, El plan deberá incluir la asignación de responsabilidades, cronograma de actividades y tiempos límite para el cumplimiento de los objetivos (Seguimiento y control).	Es necesario que la Alta dirección se comprometa para el desarrollo de esta aplicación, Hay un cambio continuo en el ambiente de seguridad que presentan riesgos, siendo las amenazas y las vulnerabilidades continuas. Para aplicar la ISO es imprescindible para la certificación realizar un diagnóstico de cómo se encuentra la empresa, una vez que se requieran certificar, la empresa deberá abordar planes de implementación, documentación, que exige la norma para verificar que la norma siga también se tendrá en cuenta el seguimiento y control.
2	¿Cómo elaborar el diagnostico de una empresa de telecomunicaciones para aplicar la norma ISO 27009?	Para un correcto diagnostico hay una serie de pasos que debemos que tener en cuenta, primero habrá que Identificar la seguridad de la información actual como las medidas de protección de la privacidad digital que se aplican para evitar el acceso no autorizado a los datos, luego se evalúan los procesos de la información necesarios para que el sistema cumpla con todos los requisitos del estándar ISO , todo esto ha impulsado una demanda de soluciones y expertos en seguridad de datos que sean capaces de construir redes más fuertes y menos vulnerables. La idea de que las infraestructuras locales son más seguras que las infraestructuras en la nube es un mito. El acceso físico no autorizado a los centros de datos en la nube es extremadamente raro. Las peores infracciones ocurren detrás de los firewalls de las empresas y de sus propios empleados. Los datos en una nube pueden residir en cualquier número de servidores en cualquier número de ubicaciones, en lugar de un servidor dedicado dentro de la red local. el cumplimiento de las políticas y leyes de privacidad, y las organizaciones deben	Para realizar un buen diagnóstico se deberá realizar algunos pasos como la identificación de la seguridad actual de la empresa, la protección de la privacidad digital, para evitar el acceso no autorizado. Se estudia los procesos de información necesario para que se cumpla los requisitos del ISO. Los expertos son capaces de construir redes más fuertes y menos vulnerables, Las infraestructuras son mas fuertes en la nube. Acceso físico no autorizado al datacenter,los firewalls son los peores centros de intuición.

		supervisar cualquier actividad sospechosa, el acceso a datos no autorizados y remediar con controles de seguridad, alertas o notificaciones a todo aquello que las entidades consideran importante o de alta validez para la misma, ya que puede contener información importante como lo puede ser bases de datos con usuarios, contraseñas, números de cuentas, etc.	
3	¿Cómo implementar la norma ISO 27009 en una empresa de telecomunicaciones?	Para la implementación de la norma deberíamos tener en cuenta las vulnerabilidades antes de diseñar un plan para solucionar las pruebas de intrusión que implican la ejecución del plan de procesos manuales o automatizados que interrumpen los servidores, las aplicaciones, las redes e incluso los dispositivos de los usuarios finales para ver si la intrusión es posible y dónde se produjo esa ruptura, para la planificación de los procesos se realiza mediante una secuencia ordenada de pasos, estos procesos de administración están diseñados para la seguridad de datos y finalmente el Plan de mejora nos permite elaborar un plan de contingencia para atacar los riesgos que aparezcan en el Proyecto y corregirlo al momento .	Se debe de tener en cuenta las vulnerabilidades antes de hacer un plan. Pruebas de intrusión que ejecutan el plan de procesos manuales, ya que esto interrumpe los hosts, aplicación, usuarios finales, etc finalmente el plan de mejora, elaborando un plan de contingencia para atacar los riesgos.
4	¿Qué riesgos existe al implementar la norma ISO 27009 en una empresa de telecomunicaciones?	Los negocios comparten una serie de riesgos comunes y contienen otros específicos de su organización. Existen algunas guías o listas que nos pueden ayudar a verificar si esos riesgos comunes que comparten la mayoría de las organizaciones nos afecta en la seguridad de la información también es necesario elaborar un plan de riesgo para tener en cuenta los métodos sofisticados para neutralizar a los intrusos porque para la ejecución del plan de riesgo se debe tener claro todas los accesos denegados para estos delitos, es por ello que se realizara una planificaremos de los procesos con ello tendremos una relación de riesgos , por lo que el plan de mejora nos ayudara para subsanar aquellos vacíos de seguridad por lo que se mejorara la eficiencia y eficacia	Se comparte una serie de riesgos típicos y otros específicos de una organización existen distintos guías que verifican los riesgos comunes iguales para ver si afectan a la seguridad de la organización. se elabora un plan de riesgos teniendo en cuenta métodos para neutralizar ataques. Por lo que el plan ayuda a subsanar esos vacíos de seguridad
5	¿Qué documentos y formatos se usan para implementar la norma ISO 27009?	El Diseño de formatos exige la identificación y descripción de procesos necesarios para que el sistema cumpla con todos los requisitos del estándar ISO, deberá incluir la asignación de responsabilidades, cronograma de actividades y tiempos límite para el cumplimiento de los objetivos ,una vez que se genera la documentación necesaria, es preciso crear un método que permita el control de los documentos, siendo un medio para gestionar la creación, aprobación, distribución, revisión, almacenamiento, modificación y	exige la identificación y descripción de procesos necesarios para que el sistema cumpla con todos los requisitos la documentación necesaria, es preciso crear un método que permita el control de los documentos

		eliminación de los diferentes documentos que se tramiten en la empresa.	
6	¿Cuáles son las estrategias del seguimiento y control?	El procedimiento de Seguimiento y Control del Proyecto establece el conjunto de acciones que se llevarán a cabo para la comprobación de la correcta ejecución de las actividades del proyecto, por lo que urge conocer la eficiencia del sistema y conocer los posibles fallos que pueden presentarse. La mejor forma de hacerlo es mediante la realización de una auditoría interna es preciso que la alta dirección haga una revisión de la labor general y verifique el cumplimiento de las acciones correctivas determinadas durante la auditoría interna luego de observar estas observaciones por parte de las auditorias realizaremos acciones Preventivas para evitar vulnerabilidades y restringir a los intrusos	El conjunto de acciones que se llevarán a cabo para las actividades del proyecto por lo que para la realización se ejecutaran auditorías por lo que la alta dirección hará una revisión de la labor general para informar al equipo responsable sobre las correcciones de las vulnerabilidades y luego realizar las acciones preventivas.

N°	PREGUNTAS	Entrevista 1: Gerente de Seguridad TDP	Entrevista
1	¿Cómo aplicar la norma ISO 27009 para prevenir riesgos del sistema de información en una empresa de telecomunicaciones?	El Para aplicar la norma se debe planificar bien y con tiempo, la planeación y la organización del proyecto representan un gran esfuerzo, por lo que influye en gran medida sobre el uso de recursos, lo expedito del proceso y el nivel de satisfacción de los empleados para el diagnóstico de la seguridad de la información debemos tener en cuenta que al investigar y analizar los riesgos asociados a los procesos del propio negocio y su entorno, una de las primeras actividades a realizar en la implementación de la norma en una empresa de telecomunicaciones es elaborar un inventario de activos que recoja cuáles son los principales activos de información en la organización, para establecer un expediente de registro de evidencias, organice la documentación solicitada, recopile actas y material relacionados con las pruebas realizadas o elaboración de formatos necesarios usar procedimientos en condiciones reales de operación para validar el diseño, la documentación e implementación del sistema de calidad.	Es necesario que la Alta dirección se comprometa para el desarrollo de esta aplicación, Hay un cambio continuo en el ambiente de seguridad que presentan riesgos, siendo las amenazas y las vulnerabilidades continuas. Para aplicar la ISO es imprescindible para la verificación realizar un diagnóstico de cómo se encuentra la empresa, una vez que se requieran certificar, la empresa deberá abordar planes de implementación, documentación, que exige la norma para verificar que la norma siga también se tendrá en cuenta el seguimiento y control.
2	¿Cómo elaborar el diagnostico de una empresa de telecomunicaciones para aplicar la norma ISO 27009?	El diagnóstico de la seguridad de la información propone un enfoque sistémico y por objetivos, aplicado a los principios básicos de evidencia, análisis, síntesis y de control ,el procedimiento para el diagnóstico se puede resumir de la siguiente forma, el diagnóstico con la definición de los objetivos, la identificación de activos y recursos, seguidamente se aplica las técnicas para evaluar los recursos disponibles, aplicando el enfoque a procesos de información para evaluar globalmente todas las áreas de la organización ,así mismo, de cada una de ellas deben verificarse diferentes aspectos básicos relacionados con la normativa vigente, la aplicabilidad al caso real de la organización, la eficiencia del control ejercido, el valor económico, la empleabilidad y la formación del personal encargado también el diagnóstico del Hardware, Software y la evaluación de las políticas de seguridad.	El diagnóstico de la seguridad de la información propone un enfoque sistémico y por objetivos, aplicado a los principios básicos el diagnóstico con la definición de los objetivos, la identificación de activos y recursos así mismo, de cada una de ellas deben verificarse diferentes aspectos básicos relacionados con la normativa vigente, la aplicabilidad al caso real de la organización, la eficiencia del control ejercido la empleabilidad y la formación del personal encargado también el diagnóstico del Hardware, Software
3	¿Cómo implementar la norma ISO 27009 en una empresa de telecomunicaciones?	La organización con respecto a los niveles de madurez requeridos, evaluar los riesgos, analizar los controles y poder determinar un plan de riesgo, para comenzar a trabajar en los procesos críticos para la organización por consiguiente la ejecución del plan para implementar la norma, el equipo encargado debe tener presente los criterios de medición y objetivos comprobados(Planificación de los procesos) ,también será necesario una serie de recomendaciones para poder incorporar un plan de mejora	evaluar los riesgos, analizar los controles y poder determinar un plan de riesgo la ejecución del plan para implementar la norma, el equipo encargado debe tener presente los criterios de medición y objetivos comprobados también será necesario una serie de recomendaciones para poder incorporar un plan de mejora
4	¿Qué riesgos existe al implementar la norma ISO 27009 en una empresa de telecomunicaciones?	Para evaluar los riesgos se debe analizar los controles y poder determinar un plan de riesgo, para comenzar a trabajar en la ejecución del plan de la organización, luego para la planificación de procesos se analiza el previo diagnóstico eficiente de seguridad de la información es por este motivo que se recomienda el análisis funcional de la organización, considerando un plan de mejora que e se encuentran inmersas dentro del ciclo de mejora continua PHVA (Planear, Hacer,	los riesgos se debe analizar los controles y poder determinar un plan de riesgo, para comenzar a trabajar en la ejecución del plan de la organización el análisis funcional de la organización, considerando un plan de mejora que e se encuentran inmersas dentro del ciclo de mejora continua PHVA (Planear, Hacer, Verificar

		Verificar y Actuar), y puede ajustarse y acomodarse al tipo de empresa a la cual se quiera aplicar.	y Actuar), y puede ajustarse y acomodarse al tipo de empresa a la cual se quiera aplicar
5	¿Qué documentos y formatos se usan para implementar la norma ISO 27009?	La Documentación de lo que se haga proporciona visibilidad del proyecto, una guía para el trabajo, una base de referencia para revisar el avance y un registro de lo realizado como referencia futura, aunque se debe evitar documentar lo innecesario, el diseño de formatos pueden iniciar con anticipación en el proyecto y son paralelas a las etapas planes de organización y calidad estos elementos se estandarizan con su documentación formal para su posterior implementación los cambios finales a la documentación y el cierre de cualquier no conformidad en la implementación se traslapan con la validación del sistema de seguridad, la cual se debe asegurar los métodos de información para su participación en el análisis, redefinición y documentación de sus labores es esencial.	proporciona visibilidad del proyecto, una guía para el trabajo, una base de referencia para revisar el avance el diseño de formatos puede iniciar con anticipación en el proyecto y son paralelas a las etapas planes de organización y calidad estos elementos se estandarizan con su documentación formal la cual se debe asegurar los métodos de información para su participación
6	¿Cuáles son las estrategias del seguimiento y control?	Contar con un sistema de seguimiento y control que funcione, que asegure una calidad consistente del producto, con los registros adecuados para verificarlo, por lo que requiere auditorías a los procedimientos, para verificar su consistencia y compatibilidad con el resto de la documentación y a las instrucciones de trabajo con el fin de verificar su adecuación con los requisitos de la norma, los procedimientos de acción correctiva y acción preventiva , facilitan el proceso de perfeccionar, diseñar, documentar e implementar los elementos del sistema de calidad, así como para solucionar las no conformidades identificadas durante la evaluación del mismo.	sistema de seguimiento y control que funcione, que asegure una calidad consistente del producto su consistencia y compatibilidad con el resto de la documentación y a las instrucciones de trabajo con el fin de verificar su adecuación con los requisitos de la norma facilitan el proceso de perfeccionar, diseñar, documentar e implementar los elementos del sistema de calidad,

N°	PREGUNTAS	Entrevista 1: Supervisor de Seguridad TDP	Entrevista
1	¿Cómo aplicar la norma ISO 27009 para prevenir riesgos del sistema de información en una empresa de telecomunicaciones?	El ambiente dinámico que presentan los riesgos de seguridad nos ofrecen cambios continuos, donde las amenazas son constantes, las vulnerabilidades son descubiertas y los incidentes de seguridad se presentan con repercusiones importantes, ya sea para diagnosticar el estado en el que se encuentra, se debe revisar las falencias y revisar cual es el estado de seguridad actual para la implementaciones la normales un aspecto clave en cualquier organización que desea alinear sus objetivos y principios de seguridad de la información, también se debe documentar todos los procesos y de ser necesario diseñar formatos para que obtengamos un mejor seguimiento y control de los procesos deben incluir la verificación de las acciones llevadas acabo	Los riesgos de seguridad nos ofrecen cambios continuos, las vulnerabilidades son descubiertas por lo que es necesario diagnosticar el estado de seguridad actual para la implementación la norma un aspecto clave es documenta todos los procesos y de ser necesario se diseñar documento necesarios ,luego se debe realizar un análisis y controlar para reducir las vulnerabilidades.
2	¿Cómo elaborar el diagnostico de una empresa de telecomunicaciones para aplicar la norma ISO 27009?	Es importante mencionar que el diagnóstico y la propuesta: la revisión preliminar de los sistemas de información, realizada por medio del internet y los conocimientos adquiridos del equipo de trabajo ayudara a recolectar información sobre la infraestructura de los equipos intermediarios como firewalls , switches o sistemas de seguridad que se encuentran corriendo, sin embargo las políticas de seguridad actuales comprender el diagnóstico de sistemas de información y la propuesta de plataforma de información y comunicación son última instancia estos fueron insumos importantes y fundamentales para el desarrollo de este proyecto de investigación	la revisión preliminar de los sistemas de información, realizada por medio del internet y los conocimientos adquiridos del equipo de trabajo ayudara a recolectar información sobre la infraestructura de los equipos intermediarios sin embargo las políticas de seguridad actuales comprender el diagnóstico de sistemas de información y la propuesta de plataforma de información comunicación son última instancia estos fueron insumos importantes y fundamentales para el desarrollo de este proyecto de investigación
3	¿Cómo implementar la norma ISO 27009 en una empresa de telecomunicaciones?	Si la empresa quiere implementar la norma ISO, puede resultar abrumador averiguar por donde comenzar por este motivo, es necesario tener un buen argumento para convencer a la dirección que implementa la norma ISO, en función del plan de riesgos y ejecución en materia de seguridad de la información que se han identificado, se desarrollan procedimientos para eliminar o, en su defecto, controlar dichos riesgos con el fin de asegurar que los procesos tengan los recursos suficientes para ser eficientes y mejorar, la dirección necesita revisar datos específicos de las actividades.	puede resultar abrumador averiguar por donde comenzar por este motivo, es necesario tener un buen argumento para convencer a la dirección que implementa la norma ISO de la información que se han identificado, se desarrollan procedimientos para eliminar o, en su defecto, controlar dichos riesgos con el fin de asegurar que los procesos tengan los recursos suficientes para ser eficientes y mejorar, la dirección necesita revisar datos específicos de las actividades.
4	¿Qué riesgos existe al implementar la norma ISO 27009 en una empresa de telecomunicaciones?	Las empresas con el fin de evitar la aparición de riesgos inesperados que puedan afectar a cualquier incidencias de seguridad deberá de elaborarse un plan de riesgos principalmente porque afecta la información y los sistemas, la solución para las incidencias de seguridad son mucho más que implementar tecnología como firewalls y gateways, antivirus, es importante tener en cuenta que el propósito de los sistemas de información y los datos que contienen es apoyar los procesos de negocios, que a su vez apoyan la misión de la organización. En un sentido muy real, la información es un elemento fundamental que apoya al negocio y su misión, y contribuye a la capacidad de una organización para sostener las operaciones.	Las empresas con el fin de evitar la aparición de riesgos inesperados que puedan afectar a cualquier incidencias de seguridad deberá de elaborarse un plan de riesgos principalmente porque afecta la información y los sistemas es importante tener en cuenta que el propósito de los sistemas de información y los datos que contienen es apoyar los procesos de negocios En un sentido muy real, la información es un elemento fundamental que apoya al negocio y su misión, y contribuye

5	¿Qué documentos y formatos se usan para implementar la norma ISO 27009?	La documentación de la norma Identifica las entradas necesarias y salidas de cada uno de los procesos de la organización determinando las secuencias e interacción de todas las actividades. debe tener un diseño de formatos según la directriz de la norma y también tendrá un formato estándar para poder registrar los datos necesarios y debe ser redactado antes que se realice la evaluación y el tratamiento de riesgos y el informe de evaluación y allí se resumen todos los resultados.	la norma Identifica las entradas necesarias y salidas de cada uno de los procesos de la organización de la norma y también tendrá un formato estándar para poder registrar los datos necesarios y debe ser redactado antes que se realice la evaluación y el tratamiento de riesgos y el informe
6	¿Cuáles son las estrategias del seguimiento y control?	Las estrategias existen para que cada extremo presente alguna sugerencia de desarrollo del sistema de información usando un marco lógico con el plan de auditoria, se debe contar con el nivel de importancia de los procesos y de las áreas que van a ser auditadas y, además, hay que tener en cuenta los resultados obtenidos de auditorías previas también es necesario definir los criterios utilizados durante la auditoría, el alcance, la frecuencia y los métodos utilizados para las acciones correctivas la organización debe velar por mantener y mejorar su sistema de seguridad de la información para realizar el levantamiento de registros los cuales deben ser legibles, identificables y trazables se toman las acciones necesarias para prevenir una posible intrusión, estas acciones se pueden realizar tanto a nivel de software (actualización del sistema), a nivel hardware (p.e. asegurar físicamente nuestro servidor) o de red (filtrado de puertos).	existen para que cada extremo presente alguna sugerencia de desarrollo del sistema de información usando un marco lógico además, hay que tener en cuenta los resultados obtenidos de auditorías previas también es necesario definir los criterios utilizados durante la auditoría para las acciones correctivas la organización debe velar por mantener y mejorar su sistema de seguridad de la información para realizar el levantamiento de registros los cuales deben ser legibles

Anexo 5: Matriz de entrevistas y conclusiones

N°	Pregunta	E1 – Jefe de Seguridad de TDP	E2 – Gerente de Seguridad TDP	E3 – Supervisor de Seguridad TDP	Similitud	Diferencias	Conclusión
1	¿Cómo aplicar la norma ISO 27009 para prevenir riesgos del sistema de información en una empresa de telecomunicaciones?	Es necesario que la Alta dirección se comprometa para el desarrollo de esta aplicación, Hay un cambio continuo en el ambiente de seguridad que presentan riesgos, siendo las amenazas y las vulnerabilidades continuas. Para aplicar la ISO es imprescindible para la verificación realizar un diagnóstico de cómo se encuentra la empresa, una vez que se requieran certificar, la empresa deberá abordar planes de implementación, documentación, que exige la norma para verificar que la norma siga también se tendrá en cuenta el seguimiento y control.	Se debe planificar bien y con tiempo, la planeación y la organización del proyecto representan un gran esfuerzo, las primeras actividades a realizar en la implementación de la norma en una empresa de telecomunicaciones es elaborar un inventario de activos que recoja cuáles son los principales activo para establecer un expediente de registro de evidencias, organice la documentación solicitada, recopile actas y material relacionados con las pruebas realizadas o elaboración de formatos necesarios	Los riesgos de seguridad nos ofrecen cambios continuos, las vulnerabilidades son descubiertas por lo que es necesario diagnosticar el estado de seguridad actual para la implementación la norma un aspecto clave es documenta todos los procesos y de ser necesario se diseñar documentos necesarios, luego se debe realizar un análisis y controlar para reducir las vulnerabilidades.	Las tres entrevistas coinciden de que para poder realizar la aplicación de la norma es necesario, diagnosticar la seguridad actual, luego de evaluar la seguridad se debe implementar la norma para ello se debe documentar todos los procesos y de ser necesario diseñar formatos, la seguridad evoluciona al igual que las vulnerabilidades es por ello que también se debe realiza el monitoreo y control para reducir estas vulnerabilidades.	En la entrevista 1 indica que la alta dirección se debe comprometer en desarrollo de la aplicación, en la entrevista 2 indica que antes se debe planificar con tiempo para qué el proyecto represente un gran esfuerzo de las primeras actividades, también debe tener un inventario de activos y en la entrevista 3 indica que los riesgos de seguridad van cambiando y es por ello que la seguridad debe ser mas robusta, para evitar la intrusión de personas no autorizadas	Se concluye que para la aplicación de la norma se debe diagnosticar la seguridad actual, para tener en cuenta que protocolos de seguridad se están ejecutando, para la implementación se debe tener en cuenta el inventario de activos lógicos y físicos, se deben documentar todos los procesos para tener evidencia de que se puede aumentar o que se debe quitar de la implementación, por ultimo se

							debe monitorear y controlar las vulnerabilidades con esto evitaremos la instrucción de personas ajenas a la compañía
2	¿Cómo elaborar el diagnostico de una empresa de telecomunicaciones para aplicar la norma ISO 27009?	Para realizar un buen diagnóstico se deberá realizar algunos pasos como la identificación de la seguridad actual de la empresa, la protección de la privacidad digital, para evitar el acceso no autorizado. Se estudia los procesos de información necesario para que se cumpla los requisitos de la ISO. Los expertos son capaces de construir redes más fuertes y menos vulnerables, Las infraestructuras son más fuertes en la nube. Acceso físico no autorizado al datacenter, los firewalls	El diagnóstico de la seguridad de la información propone un enfoque sistémico y por objetivos, aplicado a los principios básicos el diagnóstico con la definición de los objetivos, la identificación de activos y recursos así mismo, de cada una de ellas deben verificarse diferentes aspectos básicos relacionados con la normativa vigente, la aplicabilidad al caso real de la organización, la eficiencia del control ejercido la empleabilidad y la	La revisión preliminar de los sistemas de información, realizada por medio del internet y los conocimientos adquiridos del equipo de trabajo ayudara a recolectar información sobre la infraestructura de los equipos intermediarios sin embargo las políticas de seguridad actuales comprender el diagnóstico de sistemas de información y la propuesta de plataforma de información comunicación son última instancia estos fueron insumos importantes y fundamentales para el	Los entrevistados indican que primero se debe identificar la seguridad actual, para evitar la redundancia de algunos procesos, una vez identificado se evalúan los procesos de información que cumplen con la norma, es por ello que el personal cuenta con conocimiento o experiencia previa, la restricción al personal no autorizada es importante para evitar la intrusión	En la entrevista 2 propone un enfoque sistemático y por objetivos para tener una secuencia ordenado de pasos a seguir para mejorar eficiencia y el control, la entrevista 3 indica que para el diagnostico es necesario realizar una revisión preliminar de los sistemas de información y también de internet, ya que los ataques informáticos muchas veces	Para el diagnostico eficiente de una empresa se debe identificar la seguridad actual para no tener redundancia en el desarrollo, luego evaluar todos los procesos de seguridad para discernir que proceso ya no es necesario y cuales deben de integrarse , el personal responsable debe haber tenido experiencia previa o

		son los peores centros de intuición.	formación del personal encargado también el diagnóstico del Hardware, Software	desarrollo de este proyecto de investigación	física o lógica es por ello que se implementan distintas políticas de seguridad.	vienen del exterior, con proxys encapsulados.	capacitación del personal competente, la infraestructura lógica y física debe contar con soporte continuo para revisar las vulnerabilidades , también se deben de implementar políticas de seguridad con el fin de reducir riesgos.
3	¿Cómo implementar la norma ISO 27009 en una empresa de telecomunicaciones?	Se debe de tener en cuenta las vulnerabilidades antes de hacer un plan. Pruebas de intrusión que ejecutan el plan de procesos manuales, ya que esto interrumpe los hosts, aplicación, usuarios finales, etc finalmente el plan de mejora, elaborando un plan de contingencia para atacar los riesgos.	Evaluar los riesgos, analizar los controles y poder determinar un plan de riesgo la ejecución del plan para implementar la norma, el equipo encargado debe tener presente los criterios de medición y objetivos comprobados también será necesario una serie de recomendaciones	Puede resultar abrumador averiguar por donde comenzar por este motivo, es necesario tener un buen argumento para convencer a la dirección que implementa la norma ISO de la información que se han identificado, se desarrollan procedimientos para eliminar o, en su	Los entrevistados indican que para la implementación de la norma es necesario un plan de riesgos para tener mapeados los posibles riesgos, luego de ejecutar este plan, es necesario planificar los procesos de contingencia con esto lograremos	En la entrevista 1 indica que se debe de tener en cuenta las vulnerabilidades antes de hacer un plan, en la entrevista 2 evalúa y analiza los controles para determinar un plan y en la entrevista 3 indica que debe de tener un buen argumento para	Para la implementación se debe tener un plan de riesgos, para evaluar los posibles riesgos, luego de este plan, se procede a la implementación siguiendo las normas y las directrices de la ISO, en este punto es

			para poder incorporar un plan de mejora	defecto, controlar dichos riesgos con el fin de asegurar que los procesos tengan los recursos suficientes para ser eficientes y mejorar, la dirección necesita revisar datos específicos de las actividades.	tener un plan de mejora y tener la información salvaguardada.	que la alta gerencia dé el visto bueno y continuar con el flujo de la implementación de la norma.	importante tener planificado todos los procesos para poder diseñar un plan de mejora y volviendo más robusta la seguridad de la información.
4	¿Qué riesgos existe al implementar la norma ISO 27009 en una empresa de telecomunicaciones?	Se comparte una serie de riesgos típicos y otros específicos de una organización existen distintos guías que verifican los riesgos comunes iguales para ver si afectan a la seguridad de la organización. se elabora un plan de riesgos teniendo en cuenta métodos para neutralizar ataques. Por lo que el plan ayuda a subsanar esos vacíos de seguridad	Los riesgos se debe analizar los controles y poder determinar un plan de riesgo, para comenzar a trabajar en la ejecución del plan de la organización el análisis funcional de la organización, considerando un plan de mejora que e se encuentran inmersas dentro del ciclo de mejora continua PHVA (Planear, Hacer, Verificar y Actuar), y puede ajustarse y acomodarse al tipo de empresa a la cual se quiera aplicar	Las empresas con el fin de evitar la aparición de riesgos inesperados que puedan afectar a cualesquiera incidencias de seguridad deberán de elaborarse un plan de riesgos principalmente porque afecta la información y los sistemas es importante tener en cuenta que el propósito de los sistemas de información y los datos que contienen es apoyar los procesos de negocios En un sentido muy real, la información es un elemento fundamental	Los entrevistados indican que se deben analizar los riesgos que existen para la implementación, también se debe implementar un plan de procesos para cada riesgo y plan de mejora de seguridad para neutralizar a los intrusos potenciales	La entrevista 1 indica que se comparte una serie de riesgos típicos y otros específicos para la entrevista 2 indica que los riesgos se deben analizar los controles y también indica el ciclo del PHVA para la mejora continua	Es importante evaluar los riesgos de seguridad antes de la implementación de la norma una vez que se tiene los riesgos potenciales se puede ejecutar un plan de contingencia, para los riesgos encontrados para obtener una mejora continua y dar seguridad al personal que esta

				que apoya al negocio y su misión, y contribuye			implementando la norma,
5	¿Qué documentos y formatos se usan para implementar la norma ISO 27009?	Exige la identificación y descripción de procesos necesarios para que el sistema cumpla con todos los requisitos de la documentación necesaria, es preciso crear un método que permita el control de los documentos	Proporciona visibilidad del proyecto, una guía para el trabajo, una base de referencia para revisar el avance el diseño de formatos puede iniciar con anticipación en el proyecto y son paralelas a las etapas planes de organización y calidad estos elementos se estandarizan con su documentación formal la cual se debe asegurar los métodos de información para su participación	La norma Identifica las entradas necesarias y salidas de cada uno de los procesos de la organización de la norma y también tendrá un formato estándar para poder registrar los datos necesarios y debe ser redactado antes que se realice la evaluación y el tratamiento de riesgos y el informe	Los entrevistados indican que es necesario diseñar formatos para tener evidencia de los procesos ejecutados, documentos de la norma estándar que se usaran para mejorar la seguridad y los métodos de información para recoger los datos para estas documentaciones	En la entrevista 1 indica que se debe identifica y describir los procesos, la entrevista 2 indica que es una guía para el trabajo, ya que recopila los antecedentes previos, el entrevistado 3 indica que evalúa las entradas y salidas evidenciando los procesos.	Primero se diseñara los formatos, para ello se debe usar los formatos estándar establecidos en la norma para recoger todo antecedente que nos ayudara a mejorar la seguridad con ello discerniremos los métodos de información a realizar
6	¿Cuáles son las estrategias del seguimiento y control?	El conjunto de acciones que se llevarán a cabo para las actividades del proyecto por lo que para la realización se ejecutaran auditorías por lo que la alta dirección hará una revisión de la labor general para informar al	Sistema de seguimiento y control que funcione, que asegure una calidad consistente del producto su consistencia y compatibilidad con el resto de la documentación y a	Existen para que cada extremo presente alguna sugerencia de desarrollo del sistema de información usando un marco lógico, además, hay que tener en cuenta los resultados obtenidos de auditorías previas	Para el seguimiento y control es necesario contar con auditorias internas para poder ver los procesos actuales con eso se vera que acciones se	El entrevistado 1 indica que es un conjunto de acines que se llevan a cabo para, el entrevistado indica que es un sistema	Se concluye que para el seguimiento y control es necesario realizar auditorías, ya sea interna o externas para poder visualizar

		equipo responsable sobre las correcciones de las vulnerabilidades y luego realizar las acciones preventivas.	las instrucciones de trabajo con el fin de verificar su adecuación con los requisitos de la norma facilitan el proceso de perfeccionar, diseñar, documentar e implementar los elementos del sistema de calidad,	también es necesario definir los criterios utilizados durante la auditoría	podrán corregir y también las acciones a prevenir		que problemas se esta teniendo para poder corregirlas y posterior a eso prevenir posibles vulnerabilidades

Anexo 6: Guía de observación

Empresa :	TELEFÓNICA DEL PERÚ S.A.A.
Ubicación :	Jirón Domingo Martinez Luján 1130, Surquillo 15048
Área :	Security Operation Center (SOC)
Observador :	Luigi Chipulina Puelles

Redacción de lo observado sobre tres personas que trabajan dentro de la unidad de estudio, donde P1: Jefe de Seguridad de TDP, P2: Gerente de Seguridad TDP y P3: Supervisor de Seguridad TDP.

P1: Después de estar encargado de múltiples proyectos durante 10 años laborando en telefónica, es usual tener llamada de los desarrolladores de la distintas empresas, solicitando más información ya que los formatos utilizados no indican exactamente que es lo que deben de mejorar, las documentaciones de los procesos no son exactas , los manuales deben de ser mas descriptivos para que una persona que desconoce los procesos tenga un mayor entendimiento por el equipo que labora en el área, también se les toma una prueba a los miembros del equipo para saber si son capaces de afrontar riesgos de seguridad ante múltiples ataques informáticos.

P2: En el tiempo laborando en telefónica se observa que la documentación no es a adecuada, se ha solicitado al SOC que se mantengan actualizados los manuales, también en este tiempo de pandemia se a mapeado todas las ips nateadas, se han implementado algunos equipos de seguridad para reforzarla, también se ha hecho un registro de los accesos para restringir a personas no deseadas dentro del firewall, tenemos que actualizar algunas normas de seguridad para reducir los riesgos.

P3: El equipo encargado de brindar el servicio, es monitoreado mediante videos que se van creando de forma automática cada vez que se conectan remotamente por el nakina, todos los comandos ejecutados se van guardando en un registro, la asistencia del personal se obtiene mediante el tiempo de conexión de la VPN , los miembros del equipo tienen usualmente múltiples llamadas por los colaboradores de las distintas empresas para que les indiquen alguna falencias detectados, donde indican en que parte del sistema es vulnerable, solicitando al dueño de la plataforma que lo subsane , para poner en producción la plataforma; la documentación brindad muchas veces no es fácil de descifrar ya que la mayoría de usuarios son programadores y muchas veces desconocen los puertos de conexión , es por ello que se pierde tiempo informando al usuario sobre las vulnerabilidades.

De lo anterior observado se entiende que durante los distintos proyectos de telefónica se tienen problemas de documentación ya que los usuarios no tienen un análisis mas descriptivo, también desconocen algunos puertos de comunicaciones ya que no se dedican a las redes y comulaciones y solo son desarrolladores por lo que generan perdida de tiempo para darles alcance sobre aspectos básicos ,pudiendo avanzar con otros procesos necesarios; estas interrupciones son causadas a falta de actualizar algunas normas de seguridad y la documentación actual no es la adecuada.

Anexo 7: Ficha de análisis documental

Empresa	TELEFÓNICA DEL PERÚ S.A.A.
Ubicación	Jirón Domingo Martinez Luján 1130, Surquillo 15048
Area	Security Operation Center (SOC)
Observador	Luigi Chipulina Puelles

La empresa Telefónica del Perú SAA teniendo múltiples sedes a nivel mundial y establecida en distintos proyectos mundiales se observa que la documentación utilizada esta desactualizada, ya que los profesionales que salen de las distintas universidades, salen especialistas de alguna rama específica, tienen cierto conocimiento de otras ramas pero no es la adecuada como para entender temas más específicos de la seguridad de la información, esta falta de documentación adecuada trae interrupciones en el trabajo del día a día, esto también trae incomodidad a los miembros de las distintas industrias , los manuales usados están desfasados por lo que no se tiene un gran entendimiento por el personal nuevo.

Por lo anterior analizado, se debe aplicar la norma ISO 27009 para mejorar los procesos actuales, dará mejor entendimiento a los usuarios, ya que describe los distintos puertos de seguridad, en la parte de los test de vulnerabilidades indica el grado de riesgo, esto dará mayor conocimiento al personal que analizará este documento, también tendremos una seguridad mas robusta, explica cómo incluir requisitos y controles adicionales de la norma que son aplicables a sectores específicos, permitiendo lograr la coherencia en el desarrollo de esta norma de seguridad.

Por tanto para la mejora de los procesos de seguridad, tanto como denegación de servicios a intrusos o restricción de permisos a personal no autorizado es necesario esta norma ya que indica los distintos puntos de vista para mejorar la seguridad de la información, obteniendo mayor confianza para ejecutar alguna aplicación específica, también mejorar la documentación de los distintos procesos ya sea con informes gerenciales o distintos documentos necesarios para la seguridad ;también reducirá la interrupción del personal inexperto de la seguridad de la información y tendrán un mejor perfil para el desarrollo de los distintos proyectos que tengan en mente ejecutar o que estén en proceso de desarrollo

Anexo 8: Otras evidencias

Autorización

UNIVERSIDAD CÉSAR VALLEJO

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año de la Universalización de la Salud"

Lima, 7 de julio de 2020
Carta P. 367-2020-EPG-UCV-LN-F05L01/J-INT

Ing.
Jacklin Muñoz Cabrera
Jefe de proyectos
Telefónica Ingeniería de Seguridad

De mi mayor consideración:

Es grato dirigirme a usted, para presentar a CHIPULINA PUELLES, LUIGI; identificado con DNI N° 46770482 y con código de matrícula N° 6700003818; estudiante del programa de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN quien, en el marco de su tesis conducente a la obtención de su grado de MAESTRO, se encuentra desarrollando el trabajo de investigación titulado:

Aplicación de la norma ISO 27009 para prevenir riesgos del sistema de información en la empresa Telefónica, Surquillo

Con fines de investigación académica, solicito a su digna persona otorgar el permiso a nuestro estudiante, a fin de que pueda obtener información, en la institución que usted representa, que le permita desarrollar su trabajo de investigación. Nuestro estudiante investigador CHIPULINA PUELLES, LUIGI asume el compromiso de alcanzar a su despacho los resultados de este estudio, luego de haber finalizado el mismo con la asesoría de nuestros docentes.

Agradeciendo la gentileza de su atención al presente, hago propicia la oportunidad para expresarle los sentimientos de mi mayor consideración.

Atentamente,

ESCUELA DE POSGRADO UCV JEFATURA CAMPUS LIMA NORTE

Jacklin Muñoz Cabrera
Jefe de Proyectos
Telefónica Ingeniería de Seguridad
20459151584

Dr. Carlos Venturo Orbegoso
Jefe
ESCUELA DE POSGRADO
UCV FILIAL LIMA
CAMPUS LIMA NORTE

Resolución

UNIVERSIDAD CÉSAR VALLEJO

RESOLUCIÓN JEFATURAL N° 1408-2020-UCV-EPG-LN

Los Olivos, 16 de junio de 2020

VISTO:

El informe presentado por el (la) docente Dr. (a) **Dr. MARTÍNEZ LÓPEZ EDWIN ALBERTO** de la Experiencia Curricular **"Diseño y Desarrollo del Trabajo de Investigación"** del programa de ***MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN***, a la Jefatura de la Escuela de Posgrado de la Filial Lima Norte de la Universidad César Vallejo, solicitando la inscripción del proyecto de investigación:

APLICACIÓN DE LA NORMA ISO 27009 PARA PREVENIR RIESGOS DEL SISTEMA DE INFORMACIÓN EN LA EMPRESA TELEFÓNICA, SURQUILLO

presentado por el (la) estudiante:

Bach. ***CHIPULINA PUELLES LUIGI***

CONSIDERANDO:

Que, el artículo 7° del Reglamento de Investigación de Posgrado indica: *"El sistema de Evaluación de la Investigación implica el seguimiento de los trabajos de investigación, desde su concepción hasta su obtención de los resultados para su sustentación y publicación"*.

Que, el artículo 14° del Reglamento de Investigación de Posgrado indica: *"La vigencia del proyecto es un año. En caso de exceder el tiempo considerado, el interesado deberá remitirse a los procedimientos de investigación de la Escuela de Posgrado"*.

Que, el artículo 17° del Reglamento de Investigación de Posgrado indica: *"El proyecto de tesis es elaborado por un estudiante bajo la asesoría del docente metodólogo, dentro del cronograma y normatividad académica establecida y culmina, previa evaluación, con opinión favorable del docente metodólogo y la obtención de la resolución del proyecto"*.

Que, el artículo 35° del Reglamento de Investigación de Posgrado indica: *"El docente se constituye en asesor metodólogo, responsable del monitoreo y evaluación del diseño y desarrollo del proyecto de tesis"*.

Que, el (la) estudiante ha cumplido con todos los requisitos académicos y administrativos necesarios para inscribir su proyecto de tesis.

Que, el proyecto de investigación cuenta con la opinión favorable del docente metodólogo de la experiencia curricular de **"Diseño y Desarrollo del Trabajo de Investigación".**

Que, estando a lo expuesto y de conformidad con las normas estatutarias y reglamento vigente;

SE RESUELVE:

Art. 1°.- Aprobar el proyecto de tesis ***APLICACIÓN DE LA NORMA ISO 27009 PARA PREVENIR RIESGOS DEL SISTEMA DE INFORMACIÓN EN LA EMPRESA TELEFÓNICA, SURQUILLO,*** presentado por el (la) Bach. **CHIPULINA PUELLES LUIGI**, con Código: **6700003818,** el mismo que contará con un plazo máximo de un año para su ejecución.

UNIVERSIDAD CÉSAR VALLEJO

Art. 2°.- Registrar el proyecto de tesis dentro del archivo de la línea de investigación: ***AUDITORIA DE SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN,*** correspondiente al Programa de ***MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN.***

Art. 3°.- Designar al Mtro(a). Dr(a). **Dr. MARTÍNEZ LÓPEZ EDWIN ALBERTO** como asesor metodólogo del proyecto de tesis ***APLICACIÓN DE LA NORMA ISO 27009 PARA PREVENIR RIESGOS DEL SISTEMA DE INFORMACIÓN EN LA EMPRESA TELEFÓNICA, SURQUILLO***.

Regístrese, comuníquese y archívese.

ESCUELA DE POSGRADO UCV JEFATURA CAMPUS LIMA NORTE

Dr. Carlos Venturo Orbegoso
Jefe
Escuela de Posgrado – Campus Lima Norte