UNIVERSIDAD NACIONAL

SANTIAGO ANTÚNEZ DE MAYOLO

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE

INGENIERÍA DE SISTEMAS E INFORMÁTICA

"DECLARACIÓN DE APLICABILIDAD MEDIANTE LA NTP-ISO/IEC27001:2014 PARA MITIGAR LOS SINIESTROS DE LA INFORMACIÓN EN LA SUB DIRECCIÓN DE LICENCIAS DE CONDUCIR DE LA DIRECCIÓN REGIONAL DE TRANSPORTE Y COMUNICACIÓN DE ÁNCASH, 2018"

TESIS GUIADA

PARA OPTAR EL TÍTULO DE

INGENIERO DE SISTEMAS E INFORMÁTICA

AUTOR

Bach. JOSE ANTONIO QUISPE BARRETO

ASESOR:

Ing. ERICK GIOVANNY FLORES CHACÓN

HUARAZ-PERÚ

2018

PRGRAMA DE TITULACIÓN PROFESIONAL

MODALIDAD TESIS GUIADA 2018

Nº Registro: T082

DEDICATORIA

A mis padres por su gran apoyo incondicional, paciencia y amor en toda la trayectoria universitaria, a mis hermanos por su aliento de seguir adelante y a mis compañeros por su apoyo incondicional.

Jose Antonio Quispe Barreto

AGRADECIMIENTO

A mi gran asesor Erick Giovanny flores Chacón por brindarme su sapiencia en forma dosificada superando mis expectativas.

A todas las personas que contribuyeron con un granito de arena para culminar la presente investigación.

Jose Antonio Quispe Barreto

PRESENTACIÓN

Señores miembros del jurado:

Cumpliendo con las disposiciones del Reglamento de Grados y Títulos de la Escuela Profesional de Ingeniería de Sistemas e informática de la Universidad Nacional Santiago Antúnez de Mayolo, se presenta ante un ilustrado jurado la siguiente tesis: ” Declaración de aplicabilidad mediante la NTP-ISO/IEC27001:2014 para mitigar los siniestros en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash, 2018”. Siendo este requisito obligatorio para obtener el Título Profesional de Ingeniero de Sistemas e Informática.

El presente trabajo, está compuesto de los siguientes capítulos, en el capítulo I se determinó el objetivo que fue Conocer cómo la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 mitigara los siniestros de los activos de información en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash. En el capítulo II se consideró los antecedentes internacionales y nacionales en el capítulo III se definió loa materiales y métodos. En el capítulo IV se realizó un diagnóstico de la situación actual en cuanto a la gestión de riesgo. En el capítulo V se estableció el diseño de la solución en el capítulo VI la construcción de la solución y en el capítulo VII se implementa el plan en el capítulo VIII se expone los resultados en el capítulo IX se discute los resultados y finalmente las conclusiones y recomendaciones.

MIEMBROS DEL JURADO:

_____

Ing. Salazar Cáceres Rolando Roberto
Presidente
Reg. C.I.P. Nº 25976

_____

Ing. Medina Villacorta Alberto Martin
Secretario
Reg. C.I.P. Nº 143211

_____

Ing. Flores Chacón Erick Giovanny
Vocal
Reg. C.I.P. Nº 89540

RESUMEN

El propósito principal de la investigación declaración de aplicabilidad mediante la NTP-ISO/IEC27001:2014 para mitigar los siniestros en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash, fue proponer unos lineamientos de seguridad de información en el proceso de emisión de brevete.

Se tuvo en consideración las teorías de método de elipses, gestión de riesgo teniendo en cuenta las NTP – ISO/IEC 27001:2014 y sus anexos en donde esta los controles de seguridad

La investigación fue de tipo no experimental de alcance descriptivo correlacional y de corte transversal con una muestra conformada por trabajadores y usuarios se utilizó la técnica de las encuestas y el instrumento el cuestionario posterior se hizo un análisis y procesamiento de datos para poder contrastar la hipótesis.

Se concluyó que para proponer la declaración de aplicabilidad es fundamental el apoyo de la alta gerencia ya que hace un llamado de conciencia y dota de responsabilidades a los trabajadores que perteneces en el proceso de licencias de conducir quienes aportaron con gran información en el momento de evaluar los activos de información.

Palabras claves: seguridad de información, gestión de riesgo, ISO 27001

ABSTRACT

The main purpose of the investigation Proposal of the declaration of applicability through the NTP-ISO / IEC27001: 2014 to mitigate the claims in the sub direction of driver's licenses of the regional transport and communication of Ancash, was to propose some safety guidelines of information in the brevete issuance process.

Consideration was given to the theories of ellipses method, risk management taking into account the NTP - ISO / IEC 27001: 2014 and its annexes where the security controls are.

The investigation was of non-experimental type of descriptive and correlational cross-sectional scope with a sample made up of workers and users, the technique of the surveys was used and the instrument. The subsequent questionnaire was used to analyze and process the data in order to test the hypothesis.

It was concluded that to propose the declaration of applicability it is essential the support of the top management since it makes a call of conscience and gives responsibilities to the workers that you belong in the process of driving licenses who contributed with great information at the time of evaluating information assets.

Key words: information security, risk management, ISO 27001

ÍNDICE

CAPÍTULO I

GENERALIDADES

1.1. Realidad problemática

La entidad pública, Dirección Regional de Transporte y Comunicación de Áncash se observó en el área de la sub dirección de brevetes en el proceso de obtención de licencias de conducir la insatisfacción de los usuarios en los siguientes aspectos; la disponibilidad, la confiabilidad e integridad de la información. Ya que en los primeros meses del presente año se presentaron quejas ante el libro de reclamaciones en donde se suscribe; que se le da información respecto a los usuarios de forma indiscriminada sin respetar la confidencialidad de la información, por otro lado las manifestaciones de queja es sobre la información no está cuando uno realmente lo necesita las ventanillas están cerradas en hora de trabajo impidiendo la disponibilidad de la información y por ultimo las quejas que se declaro es sobre los datos mal escritos por parte de los trabajadores faltando a la integridad de la información.

Si tal panorama sigue persistiendo es muy probablemente en un cercano futuro se pierda la información que es relevante para dicho proceso y la reputación de la entidad se desmorone trayendo sanciones no solo a los trabajadores del proceso sino también de acuerdo a norma será sancionado el director de la dirección

regional de transporte y comunicación de Áncash (Oficina nacional de gobierno electrónico e informática, 2016).

Bajo este contexto, la presente investigación, fue sobre declaración de aplicabilidad mediante la NTP-ISO/IEC27001:2014 para mitigar los siniestros en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Ancash, 2018. Específicamente en el proceso de obtención de brevete, de tal forma, que el documento resultante sirva como referencia para la implementación de la norma NTP ISO/IEC 27001:2014 ya que esta entidad pública pertenece al Sistema Nacional de Informática y por lo tanto está obligada a no solo elaborar un plan sino también a implementarla todo esto bajo el marco de las leyes peruanas (El peruano, 2016). con el afán de coadyuvar al avance del gobierno electrónico.

1.2. Enunciado del problema

1.2.1. Problema general

¿Cómo la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 mitigara los siniestros de los activos de información en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash?

1.2.2. Problemas específicos

¿De qué manera la declaración de aplicabilidad mitigara el daño de los siniestros de la información mediante el contexto de la organización de la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash?

¿De qué manera la declaración de aplicabilidad mitigara el daño de los siniestros de la información mediante la planificación de la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash?

¿Cómo será la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash?

1.3. Hipótesis

1.3.1. Hipótesis general

Con la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 se mitigará los siniestros de los activos de información en la subdirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash.

1.3.2. Hipótesis nula

Con la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 no se mitigará los siniestros de los activos de información en la subdirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash.

1.4. Objetivos

1.4.1. Objetivo general

Conocer cómo la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 mitigara los siniestros de los activos de información en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash.

1.4.2. Objetivos específicos

Establecer de qué manera la declaración de aplicabilidad mitigara el daño de los siniestros de la información mediante el contexto de la organización de la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash.

Establecer de qué manera la declaración de aplicabilidad mitigara el daño de los siniestros de la información mediante la planificación de la NTP-

ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash

Elaborar la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash.

1.5. Justificación

1.5.1. Desde el punto de vista social

Mediante la presente investigación busca dar disponibilidad, confidencialidad e integridad a la información trayendo consigo beneficios a los usuarios es decir a la sociedad también coadyuvar al avance del gobierno electrónico que es cerrar brechas digitales entre la sociedad y la tecnología.

1.5.2. Desde el punto de vista del aporte al conocimiento

La presente investigación busca, mediante la aplicación de la NTP ISO/IEC 27001:2014 referente a la gestión de riesgo, concretizar conocimientos con el objetivo de llenar vacíos para poder fortalecer los conocimientos por parte del investigador y la entidad interesada que en este caso es la dirección regional de transporte y comunicación de Ancash.

1.5.3. Desde el punto de vista normativo

La presidencia de consejo y ministros atreves de la oficina nacional del gobierno electrónico e informático es responsable de modernizar el estado para lo cual se elaboró un plan de gobierno electrónico donde existe un portafolio de proyectos unos de estos proyectos es el diseño e implementación del sistema gestión de seguridad de la información en las entidades pertenecientes al sistema nacional de informática para impulsar esta implementación se elabora la NTP-ISO/IEC 27001:2014 en el año 2016 del mes enero. En tal sentido se pretende el desarrollo de la tesis cumplir con la documentación de norma exigida para así contribuir también con la modernidad del estado.

1.5.4. Desde el punto de vista metodológica

La presente investigación busca aplicar la NTP-ISO/IEC 27001 referente a la gestión de riesgo para lo cual la piedra angular es el cálculo de riesgos en tal sentido es de mi interés conocer una metodología de acuerdo a los alineamientos de dicha norma para minimizar los riesgos de activo de información pero más que eso sería cumplir con la norma, no con toda pero con una parte de la documentación en el de la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash.

1.6. Limitación

La presente investigación tiene limitación en los siguientes aspectos:

- El jefe de la subdirección de licencias de conducir es muy estricto en temas de manipulación de la variable en el área, es decir armar un escenario para la presente investigación
- Falta de disponibilidad de compromiso del área de tramites de licencias de conducir en líneas contribuir información

En tal sentido la presente investigación solo queda en una mera investigación descriptiva sin intención de implementar.

1.7. Descripción y sustentación de la solución

La propuesta de la declaración de aplicabilidad según la norma técnica peruana ISO/IEC 27001 del 2014 es un conjunto de directrices que tiene por objetivo minimizar los siniestros de los activos de la información del área de la subdirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash.

La solución se hará mediante una metodología basada en la norma técnica peruana ISO/IEC 27001:2014 que es una secuencia de pasos que comienza con los activos de información y culmina con la declaración de aplicabilidad.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes

a) A nivel internacional

Aranda (2009) en su tesis “Implementación del primer sistema de gestión de seguridad de la información, en el ecuador, certificado bajo la norma ISO 27001:2005 ” tuvo como objetivo el desarrollo e implementación de la norma ISO 27001 y lograr la certificación para gestionar los riesgos identificados en una empresa Ecuatoriana autorizada como carrier cuyo negocio es proveer servicio de telecomunicaciones mediante una metroethernet y cuyo mercado corporaciones proveedores de internet, entidades financieras entre otros. En el desarrollo de la investigación se optó por el modelo del ciclo de Deming exigida por el estándar ISO 27001:2005 que consiste en cuatro fases: planificar, hacer, monitorear, actuar en la cual se obtuvo resultados en cada fase como por ejemplo en la fase de plan: se identificó los procesos, se utilizó el método de las elipses se tazaron los activos se usó una metodología para el análisis y evaluación de riesgos, se planteó un plan de tratamiento de riesgos, requisitos documentales y se tomaron en cuenta los factores de éxito para la fase 2 de igual manera se obtuvieron resultados como implementación del plan de controles y la capacitación de los trabajadores involucrados en la área limitada del SGSI en la tercera fase se obtuvieron resultados como el monitoreo, auditorías internas y en la cuarta fase se obtuvo

resultados como tomar reacciones a partir de lo encontrado en la tercera fase y por ultimo para lograr la certificación ISO 27001:2005 se hicieron las auditorias pertinentes y se hizo un presupuesto del costo para el proceso del certificado. Concluyendo que la norma ISO 27001:2005 está orientada al tratamiento de la seguridad de la información mediante la gestión del riesgo, también existe políticas jerárquicas donde se debe impulsar desde la gerencia para que tenga mayor éxito y los objetivos del SGSI deben estar alineados a los de negocio y por último el eslabón más débil del SGSI son las personas. Bueno esta tesis es completa ya que llego hasta el certificado y por tanto es de admirar el gran trabajo del investigador y por tanto mi tesis es un parte de todo el ejemplar y aporta a mi tesis en cuanto los factores de éxito que hay que tener en cuenta para que un SGSI cumpla con los objetivos planteados.

Buenaño y Granda (2009) en su tesis "Planeación y diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001-27002" tuvo como objetivo establecer cuáles serían los mecanismos adecuados para mitigar los riesgos asociados al uso de la información, de los sistemas y servicios informáticos utilizados por el personal de la sede Guayaquil de la Universidad Politécnico Salesiana, concluye que con una política bien estructurada los controles permiten mejorar los niveles de seguridad ya sea en s parte física, estructural, tecnológica y en su parte metódica documental.

b) A nivel nacional

Aguirre (2014) es su tesis “Diseño de un Sistema de Gestión de Seguridad de la Información para Servicios Postales del Perú”, esta tesis tuvo como objetivo Diseñar un Sistema de Gestión de Seguridad de la Información según lo indicado por la NTP ISO/IEC 27001:2008 y la NTP ISO/IEC 17999:2007 de seguridad de la información para SERPOST una empresa situada en el Perú dedicada al servicio de correspondencia, giros postales y al mercado de envíos y encomiendas nacionales e internacionales. Se desarrolló usando los lineamientos de la NTP-ISO/IEC 27001:20008 en la etapa de diseño se empezó con elaborar con las documentaciones exigidas por la norma seguidamente se valorizaron los activos de información de la mano la elabora la evaluación de riesgos y por último elabora la lista de controles para mitigar los riesgos detectados. Concluyen que solo para la etapa del diseño del SGSI fue necesario él apoye de la alta gerencia y que es necesario difundir las normas de seguridad de la información a todos los trabajadores de área y que se necesita contratar a personas especializado para dar soporte a los procesos involucrados del SGSI y que es necesario mejorar el área de logística para adquirir los controles del tratamiento del riesgo para los activos de información. Esta tesis se relaciona con la mía porque ambos abarcan solo hasta el diseño del SGSI donde contribuye en mi investigación con el uso de la herramienta Bizagui para el modelamiento de procesos utilizando la notación BPM.

Ángeles (2011) en su tesis “Sistema de Gestión de Seguridad de la Información ISO 27001 para un Data Center”, esta tesis tuvo como objetivo dar a conocer como es el proceso de implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) y la acreditación con la certificación ISO 27001 en una empresa dedicada a la prestación de servicios Outsourcing y Data Center de TI en lima, Perú.se desarrollo usando la metodología de la ISO 27001 en donde especifica el ciclo de Deming Mejora Continua donde tiene 4 etapas; la primera etapa Plan se adoptó la política de seguridad de información de la organización, se definió una metodología de Análisis de riesgo así mismo para la evaluación de riesgo. En la segunda etapa hacer se implementaron los controles de acceso físicos y lógicos, se asignaron responsabilidades y se creó el comité de seguridad, se realizaron cursos de concientización de seguridad le la información al personal. En la tercera etapa Verificar se superviso en el interior y el exterior del perímetro de gestión, el comité de seguridad evalúa la eficacia del SGSI mediante las auditorias. En la cuarta etapa Actuar el comité de seguridad identifico las mejoras que se puedan aplicar en el SGSI. Concluyen que el SGSI asegura la disponibilidad de los servicios, las cuales serán protegidas de tal manera que se conserve la integridad y confidencialidad de la información. Sin lugar a duda llegar hasta la certificación es un logro que pocos llegan para lo cual tuvo que pasar por las cuatro etapas donde se relaciona con mi tesis en la etapa de plan donde me contribuye con el análisis y evaluación de riesgo ya que es la piedra angular de mi investigación.

Romero (2006) en su tesis “Plan de Seguridad Informática en el MTC”, esta tesis tuvo como objetivo implementar el sistema de seguridad informática que permita asegurar la confidencialidad, la integridad y disponibilidad de los sistemas informáticos de modo tal que la información sea accesible solo a aquellos usuarios autorizados; garantizando así la continuidad del servicio tratando de minimizar la vulnerabilidad de los sistemas a fin de proteger la red del MTC y sus recursos de ataques internos y externos. Se desarrolló primero dando un diagnóstico de la situación actual de la seguridad de la información del MTC, seguidamente las vulnerabilidades de la infraestructura de la red de datos del MTC, evaluando el riesgo e impacto de su probable ocurrencia, seguidamente se estableció procedimientos, políticas y mecanismos técnicos para atenuar o eliminar los riesgos, seguidamente se analizó las herramientas de seguridad del MTC para posteriormente proponer una solución de seguridad de la red de datos, seguidamente se propuso políticas de seguridad informática internas basadas en la política y estándares sugeridos por la Norma Técnica Peruana y finalmente se propuso la adquisición de los recursos de seguridad informática. Concluyendo que la seguridad informática se basa, principalmente en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos y políticas de seguridad. Esta tesis se relaciona con la mía porque es una parte de la seguridad de la información donde contribuye en mi investigación con el uso de la norma técnica peruana para la elaboración de las políticas.

c) A nivel local

Mory, (2015) en su tesis "Aplicación de la norma ISO/IEC 27001 para mejorar la seguridad de la información en la empresa HM Contratistas S.A." Esta tesis tuvo objetivo principal Diseñar un Sistema de Gestión de Seguridad de Información (SGSI) siguiendo las normas internacionales ISO/IEC 27001 para mejorar la seguridad de información en la empresa HM CONTRATISTAS S.A. de la ciudad de Huaraz, se desarrolló usando la metodología de la ISO 27001 en donde especifica el ciclo de Deming Mejora Continua donde tiene 4 etapas la primera etapa Plan se identificó y realizo la valoración de activos de información de acuerdo al alcance seguidamente se procedió a identificar, analizar y evaluar los riesgos de los cuales están expuesto los activos de información seguidamente se elaboró la documentación requerida por la norma ISO/IEC 27001 y por último el modelado de los procesos de negocio para delimitar el alcance del SGSI. Las demás etapas no se llegaron a tocar porque la tesis solo consiste en la etapa del diseño. Llegando a la conclusión que la empresa no cuenta con un comité responsable de seguridad de información que estructure un plan estratégico encaminado a proteger los activos de información así mismo de las políticas controles y amenazas. Esta tesis se relaciona con la mía porque ambos abarcan solo hasta el diseño del SGSI donde contribuye en mi investigación en la etapa de Análisis utilizando para ello el FODA.

2.2. Teorías que sustentan el trabajo

Para la presente investigación se tocaron dos ítems de la norma técnica peruana ISO/IEC que son el contexto de la organización y la planificación.

a) Declaración de aplicabilidad

Declaración de aplicabilidad es un documento que se trata cómo usted implementará una gran parte de su sistema de seguridad de la información.

De hecho, la Declaración de aplicabilidad es el nexo principal entre la evaluación y el tratamiento del riesgo y la implementación de su sistema de seguridad de la información. El objetivo de este documento es definir cuáles de los 133 controles (medidas de seguridad) sugeridos en el Anexo A de la norma ISO 27001 son los que usted implementará y, para los controles que correspondan, cómo se realizará su implementación (NTP-ISO/IEC 27001,2014).

b) NTP-ISO/IEC 27001:2014 Tecnología de la información. Técnicas de la seguridad. Sistemas de gestión de seguridad de la información. Requisitos

Las Normas Técnicas Peruana son documentos que tiene como característica mejorar la calidad de proceso, producto o servicio, que para nuestro caso mejorara la calidad de proceso de entrega de brevetes de la D.R.T.C.A. las NTP son normalmente de carácter voluntario, pero para nuestro caso es de carácter obligatorio de acuerdo al Plan Nacional del Gobierno Electrónico 2012-2017.

Las NTP-ISO/IEC 27001:2014 son una copia adaptada a nuestra realidad Peruana del Estándar ISO/IEC 27001 Reino Unido de Gran Bretaña que está orientada a la seguridad de la información.

El sistema de gestión de la seguridad de la información preserva la confiabilidad, integridad y disponibilidad de la información aplicando procesos de gestión de riesgos y proporciona confianza a las partes interesadas en el sentido en que los riesgos sean manejados adecuadamente. Es importante que es sistema de gestión de la seguridad de la información se parte de y este integrado con los procesos de la organización y la estructura de gestión gerencial y que la seguridad de la información se considere en el diseño de proceso, sistemas y controles de la información. Se espera que la implementación de un sistema de gestión de seguridad de la información crezca a escala en concordancia con las necesidades de la organización (NTP-ISO/IEC 27001,2014).

b.1) Contexto de la organización

Para comprender el contexto de la organización la NTP-ISO/IEC 27001:2014 indica 3 ítems las cuales se detallarán a continuación:

b.2) Comprender la organización y su contexto

La organización debe determinar los aspectos externos e internos que son relevantes para este propósito y que afecten su capacidad de lograr el(los) resultado(s) deseados de este sistema de gestión de seguridad de la información.

b.3) Comprender las necesidades y expectativas de las partes interesadas

La organización debe de determinar 2 aspectos que se detallan a continuación:

El primero las partes interesadas relevantes al sistema de gestión de seguridad de la información. El segundo los requisitos de estas partes interesadas relevantes a la seguridad de la información.

b.4) Determinar el alcance del sistema de gestión de seguridad de la información

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance, en tal sentido se debe considerar los siguientes aspectos:

Primero los aspectos externos e internos referidos a comprender la organización y su contexto, segundo los requisitos referidos a comprender las necesidades y expectativas de las partes interesadas y por último identificar las interfaces y dependencias entre actividades realizadas por la organización y las que son realizadas por otras organizaciones (NTP-ISO/IEC 27001,2014).

b.5) Planificación

Las acciones que deben de realizarse para tratar el riesgo y las oportunidades son mencionadas a continuación:

Considerar los asuntos referido al contexto de la organización, determinar los riesgos y oportunidades que necesitan ser tratados para asegurar que el sistema de gestión de seguridad de la información pueda lograr su resultado esperado y lograr la mejora continua (NTP-ISO/IEC 27001,2014).

b.6) Valoración del riesgo de seguridad de la información

El término valoración alude dos términos el análisis y la evaluación del riesgo la cual cada uno de estos factores tienen sus propios ítems que se menciona a continuación:

En el primer factor análisis se deben identificar los activos de información, identificación de los requerimientos legales y comerciales que son relevantes para los activos identificados, la tasación de los activos identificados considerando los requerimientos legales y comerciales así como los impactos resultantes de una perdida por confidencialidad, integridad y disponibilidad, identificación de amenazas y vulnerabilidades para cada activo previamente identificado y cálculo de posibilidades de que las amenazas y vulnerabilidades ocurran (NTP-ISO/IEC 27001,2014).

En el segundo factor la evaluación se debe considerar el cálculo del riesgo y la identificación de los significados de los riesgos.

b.7) Tratamiento de riesgo

La organización debe definir y aplicar un proceso de tratamiento de riesgo de seguridad de la información para lo cual debe:

Primero debe Seleccionar opciones de tratamiento de riesgo de la seguridad de la información apropiadas, tomando en cuenta los resultados de la valoración de riesgo. Segundo determinar los controles necesarios para posteriormente implementar las opciones elegidas de tratamiento de riesgo de seguridad de la información. Tercero comparar los controles determinados en el paso anterior con aquellos del Anexo A y verificar que no se omitido ningún control y cuarto producir una declaración de aplicabilidad que contenga los controles necesarios del Anexo A (NTP-ISO/IEC 27001,2014).

b.8) Método de las elipses

Esta metodología permite, con gran precisión, poder identificas posteriormente los activos de información. Permite dado un determinado alcance de un SGSI, identificar sus interfaces, interdependencias con áreas y procesos, así como averiguar el tipo de información que fluye y los grados de acuerdo que existe. El método de las elipses se utiliza como fuente de inspiración para deriva posteriormente los activos de información. Al analizar los procesos identificados

y el flujo de información procede a identificar los activos de información (Alberto, 2007).

b.9) Identificación de activos

En sentido estricto un activo es algo a lo que una organización directamente le asigna un valor y, por tanto, la organización debe protegerla. Con base al resultado de la metodología de las elipses se deben identificar los activos de información clasificándola en los siguientes aspectos Activos de información (datos, manuales entre otros), documento de papel(contrato), activos de software (sistemas, aplicaciones entre otros), activos físicos (computadoras, USB entre otros), personal (clientes, personal), imagen de compañía, servicios (internet, línea de teléfono entre otros) (Alberto, 2007).

b.10) Requerimientos legales

Al identificar los activos de información, se debe analizar si existen requerimientos legales y comerciales relacionados con los activos identificados. Si hubiera requerimientos legales o comerciales, se deben resisar si dichos requerimientos legales o comerciales involucran otros activos de información (Alberto, 2007).

b.11) Tasación de activos

Es darle un valor a cada activo identificado, tomando en cuenta 3 aspectos, la confidencialidad integridad y disponibilidad para lo cual se usará una escala como por ej. Likert que toma valores de 1 que significa muy poco hasta valores como 5 que significa muy alto y el valor final de cada activo se sacará por ej. Con el promedio o el valor máximo de los tres aspectos tomados en cuenta (Alberto, 2007).

b.12) Identificación de ocurrencia de las amenazas

Una amenaza es una indicación de un evento desagradable con el potencial de causar daño. Entonces se identificara las distintas amenazas que puedan afectar a un activo y se clasificara teniendo en cuenta 6 tipos de amenazas que son; amenaza natural, amenaza a instalaciones, amenazas humanas amenazas tecnológica, amenazas operacional y amenazas social y posteriormente se debe evaluar la posibilidad de ocurrencia del susodicho; para lo cual se tendrá que tener una estadística o un juicio de experto que tengan conocimiento de la naturaleza de la amenaza y pueda clasificarla en una escala de Likert (Alberto, 2007).

b.13) Identificación de las vulnerabilidades

Las vulnerabilidades son las debilidades del sistema de seguridad por sí misma no causan daño, simplemente son condiciones que pueden hacer que una amenaza afecte un activo. Entonces se identificará las distintas vulnerabilidades que puedan afectar a un SGSI y se clasificara teniendo en cuenta 5 tipos de vulnerabilidades que son: seguridad de los recursos humanos, control de acceso, seguridad física y ambiental, gestión de operaciones y comunicaciones y por último mantenimiento desarrollo adquisición de sistemas de información (Alberto, 2007).

b.14) Cálculo de amenazas y vulnerabilidades

Es el cálculo de la posibilidad de que puedan juntarse la amenaza y la vulnerabilidad por tanto causar un riesgo, que también se denomina probabilidad de ocurrencia. Entonces Una vez identificados las vulnerabilidades, por cada una de ellas, se debe evaluar la posibilidad de que sean explotados por las amenazas. Para este propósito se podría utilizar una escala de Likert, por tanto, hay una relación entre amenaza y vulnerabilidad y la pregunta guía seria ¿Qué amenaza pudiese explotar cuál de las vulnerabilidades? Y también tomando en cuenta de las amenazas los siguientes aspectos: amenaza deliberada, amenaza accidental, incidente del pasado y por último nuevos desarrollo y tendencias (Alberto, 2007).

b.15) Análisis del riesgo y su evaluación

Se analizará el riesgo en una tabla con las siguientes columnas activo, amenaza, impacto de amenaza, probabilidad de ocurrencia, medición del riesgo y por último priorización. En donde la columna impacto de amenaza se obtendrá tasándola en una escala de Likert teniendo en cuenta por ej. Lo económico, la columna de medición de riesgo se puede calcular con la multiplicación de las columnas impacto de amenaza y probabilidad de ocurrencia y por último la columna priorización se puede utilizar rangos para poder clasificarla en una escala de Likert (Alberto, 2007).

b.16) Tratamiento de riesgo y el proceso de toma de decisión gerencial

Una vez que el riesgo se ha calculado, se debe iniciar el proceso de toma de decisiones con respecto a cómo se tratar el riesgo, para lo cual hay 4 opciones que son; reducir el riesgo, objetivamente aceptar el riesgo, transferencia del riesgo y evitar el riesgo. Para tomar esta decisión se tendrá 2 aspectos clave que son; el posible impacto si el riesgo se pone en manifiesto y que tan frecuente puede suceder por otra parte quien toma las decisiones son la alta gerencia con la ayuda del especialista en SGSI (Alberto, 2007).

b.17) Selección de objetivos de control y controles para el tratamiento de riesgo

Una vez se realiza el proceso de identificar las opciones de tratamiento del riesgo y haberlas evaluado, la empresa debe decidir qué objetivos de control y controles debe escoger para el tratamiento de riesgo. Los controles según ISO/IEC 27001:2014 están en el anexo A de dicha NTP (Alberto, 2007).

b.18) Siniestro de activo de información

Es un suceso que produce un daño de consideración en los activos de información que puede ser por perdida, robo, inadecuada tratamiento de la información entre otros (Merino C. y Cañizares R., 2011).

2.3. Definición de términos

Los conceptos mostrados se encuentran en la norma ISO/IEC 27000 definición de vocabulario.

a) Activo

"Algo que tenga valor para lo organización. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos" (ISO/IEC 27000, 2014).

b) Amenaza

"Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización" (ISO/IEC 27000, 2014).

c) Análisis de riesgos

"Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización" (ISO/IEC 27000, 2014).

d) Confidencialidad

"Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados" (ISO/IEC 27000, 2014).

e) Control

"Herramienta de la gestión del riesgo, incluido: políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal" (ISO/IEC 27000, 2014).

f) Disponibilidad

"Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados" (ISO/IEC 27000, 2014).

g) Enunciado de aplicabilidad

"Enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la organización" (ISO/IEC 27000, 2014).

h) Integridad

"Propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada" (ISO/IEC 27000, 2014).

i) Impacto

"Consecuencia que sobre un activo tiene la materialización de una amenaza" (ISO/IEC 27000, 2014).

J) Incidente de seguridad de información

"Es indicado por una o varias series s de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de negocios y de amenazar la seguridad de información" (ISO/IEC 27000, 2014).

k) ISO

"Organización de Estandarización Internacional" (ISO/IEC 27000, 2014).

l) Mitigar

"Disminuir la intensidad, la gravedad o la importancia de algo" (ISO/IEC 27000, 2014).

m) Norma

"Regla o conjunto de reglas que hay que seguir apara llevar a cabo una acción, p orque está establecido o ha sido ordenado de ese modo" (ISO/IEC 27000, 2014).

n) Riesgo

"Es un problema potencial que puede ocurrir dentro de una organización" (ISO/IEC 27000, 2014).

o) Riesgo residual

"Riesgo que se da tras la aplicación de salvaguardas dispuestas en un escenario de simulación o en el mundo real" (ISO/IEC 27000, 2014).

p) Salvaguarda

"Procedimiento o mecanismo tecnológico que reduce el riesgo" (ISO/IEC 27000, 2014).

q) Seguridad de la información

"Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables. Preservación de la confidencialidad, integridad y disponibilidad de la información, así mismo, otras propiedades como la autenticidad, no rechazo, contabilidad y confiabilidad también pueden ser consideradas" (ISO/IEC 27000, 2014).

r) SGSI

"Sistema de Gestión de Seguridad de la Información. Es una herramienta de gestión" (ISO/IEC 27000, 2014).

s) MRTCA

"Ministerio Regional de Transporte y comunicación de Ancash" (ISO/IEC 27000, 2014).

t) Vulnerabilidad

"Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza. Propiedades intrínsecas de que algo se produzca como resultado de una sensibilidad a una fuente de riesgo que puede conducir a un suceso con una consecuencia" (ISO/IEC 27000, 2014).

v)Acción correctiva

"Acción para eliminar las causas de una no conformidad y prevenir su repetición" (ISO/IEC 27000, 2014).

w) Acción preventiva

"Medida de tipo pro-activo orientada a prevenir potenciales no conformidades" (ISO/IEC 27000, 2014).

x) Aceptación de riesgo

"Decisión informada de asumir un riesgo concreto" (ISO/IEC 27000, 2014).

CAPÍTULO III

MATERIALES Y METÓDOS

3.1. Materiales

a) Los laboratorios usados en la presente investigación se detallan en el siguiente cuadro.

CUADRO N°3.1

LABORATORIOS DISPONIBLES

Local	Ambiente
UNASAM	Biblioteca central
DRTCA	Área de tramites

Fuente: Elaboración propia.

b) Los softwares que se usó fueron en la presente investigación se detallan en el siguiente cuadro.

CUADRO N°3.2

SOFTWARE EMPLEADO

Software	Descripción	Tipo de licencias
Ms Word	Herramienta para la elaboración del proyecto de tesis	Versión trial
Ms Excel	Herramienta para los resultados	Versión trial
Ms Project	Herramienta para el cronograma del proyecto	Versión trial
Ms Visio	Herramienta para los diagramas	Versión trial

Fuente: Elaboración Propia

c) Los recursos computacionales que se usó fueron en la presente investigación se detallan en el siguiente cuadro.

CUADRO N°3.3

RECURSOS COMPUTACIONALES

Nombres	Características
Computadora portátil	Procesador: Core i5 Memoria RAM: 16 GB Disco duro: 1 TB Sistema operativo: Windows 10
USB	Arquitectura: 3.0

Fuente: Elaboración propia.

3.1.1. Población

La población es el Gerente, los trabajadores y los clientes de la Dirección Regional de Transporte y Comunicación de Áncash en el año 2018, como se muestra en la siguiente tabla

CUADRO N°3.4

POBLACIÓN

N°	Descripción	Población total
1	Trabajadores	35
2	Clientes	90

Fuente: Sub Dirección de Licencias de Conducir

Hay que tener en cuenta que el Gerente se incluye a los trabajadores que participan en el proceso de entrega de brevetes y los clientes en la Sub

Dirección de Licencias de Conducir de la Dirección Regional de Transporte y Comunicación de Áncash.

3.1.2. Muestra

CUADRO N°3.5

MUESTRA 1

N°	Descripción	Población	Muestra
1	Trabajadores	35	35
	Total		35

Fuente: Elaboración Propia.

Muestra 1: Tamaño de muestra para una proporción; siendo el tamaño de muestra igual a 35 para la población de clientes, teniendo en cuenta un nivel de confianza del 95%, error de muestreo de 5% y uso de la fórmula general.

Tamaño de muestra de la población:

$$n = \frac{NZ^2PQ}{e^2(N-1) + Z^2PQ}$$

Donde:

N=35 (Población),

Z=1.96 (Nivel de confianza del 95%),

P=0.5 (Proporción de éxito),

Q=0.5 (Proporción de fracaso) y

e=0.05 (Margen de error).

CUADRO N°3.6

MUESTRA 2

N°	Descripción	Población	Muestra
1	Clientes	90	73
	Total		73

Fuente: Elaboración Propia.

Muestra 2: Tamaño de muestra para una proporción; siendo el tamaño de muestra igual a 73 para la población de clientes, teniendo en cuenta un nivel de confianza del 95%, error de muestreo de 5% y uso de la fórmula general

Tamaño de muestra de la población:

$$n = \frac{NZ^2PQ}{e^2(N-1) + Z^2PQ}$$

Donde:

N=90 (Población),

Z=1.96 (Nivel de confianza del 95%),

P=0.5 (Proporción de éxito),

Q=0.5 (Proporción de fracaso) y

e=0.05 (Margen de error).

3.2. Métodos

El diseño de investigación que se usó para contrastar las hipótesis para este caso de estudio descriptivo correlacional de dos variables la variable independiente es la NTP-ISO/IEC 27001 y la variable dependiente siniestra de la información es mediante el uso de la estadística inferencial, es decir se usará spearman para la contrastación de la hipótesis También para cumplir con los objetivos y dar respuesta a la pregunta de investigación se usará en método científico.

3.3 Técnicas

3.1.1. Fuentes de datos

Fuentes de datos para recolectar información fue la fuente primaria ya que el investigador obtuvo la información atreves de escritos por los participantes del proceso de emisión de brevete.

3.1.2. Técnica de recolección de datos

La técnica que se uso es la encuesta “es una técnica para la investigación social por excelencia, debido a su utilidad, versatilidad, sencillez y objetividad de los datos que con ella se obtiene” (Carrasco, 2013). La encuesta fue aplicada una sola vez a los trabajadores del proceso de emisión de brevetes teniendo en cuenta la muestra de la presente investigación.

3.1.3. Instrumento de recolección de datos

El instrumento que se uso es el cuestionario “es el instrumento de investigación social más usado […] ya que permite una respuesta directo. Mediante la hoja de pregunta que se le entrega a cada una de ellas. Las preguntas estandarizadas se preparan con anticipación y previsión” (Carrasco, 2013). El cuestionario se aplico una vez en el tiempo a todos los trabajadores del proceso de emisión de brevete.

3.1.4. Análisis de datos

Los datos fueron analizados con en el programa SPSS usando la estadística inferencial y está representado en el capítulo VIII en tablas.

3.4. Procedimiento

Paso 1: comprender la organización y su contexto

Poso 2: comprender las necesidades y expectativas de las partes interesadas

Paso 3: determinar el alcance del sistema de gestión de seguridad de la información

Paso 4: valorizar el riesgo

Paso 5: tratamiento del riesgo

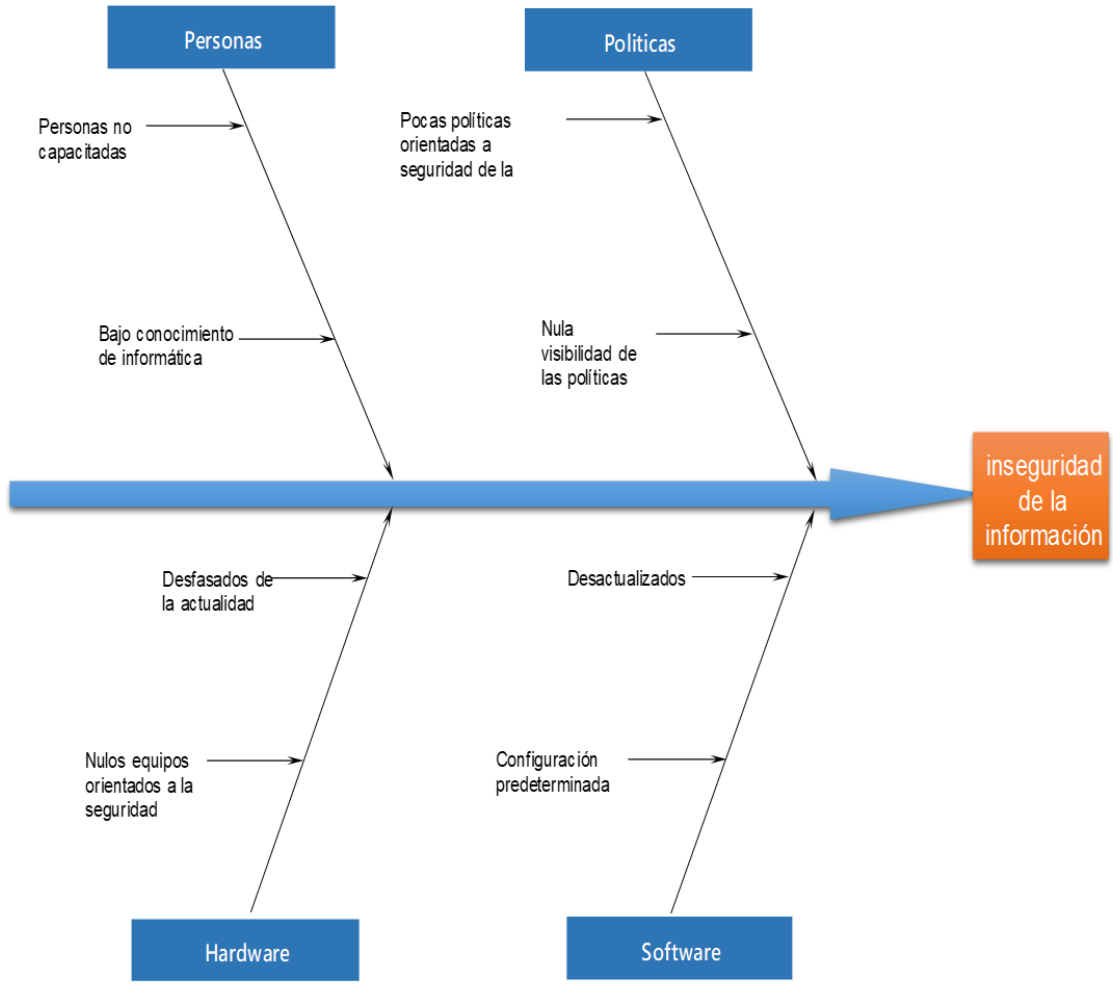
CAPÍTULO IV

ANÁLISIS

4.1 Análisis de la situación actual

GRÁFICO N° 4.1

DIAGRAMA DE ISHIKAWA



Fuente: elaboración propia

En el diagrama de Ishikawa muestra que en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash, cuenta

con personas, poco capacitadas en informática, también no se cuenta con políticas de seguridad de la información, los hardware que se usas en algunas oficinas son actualizados y en otras no, pero todos los softwares no están actualizados todo ello trayendo el efecto de la inseguridad de la información.

4.2 Identificación y descripción de requisitos

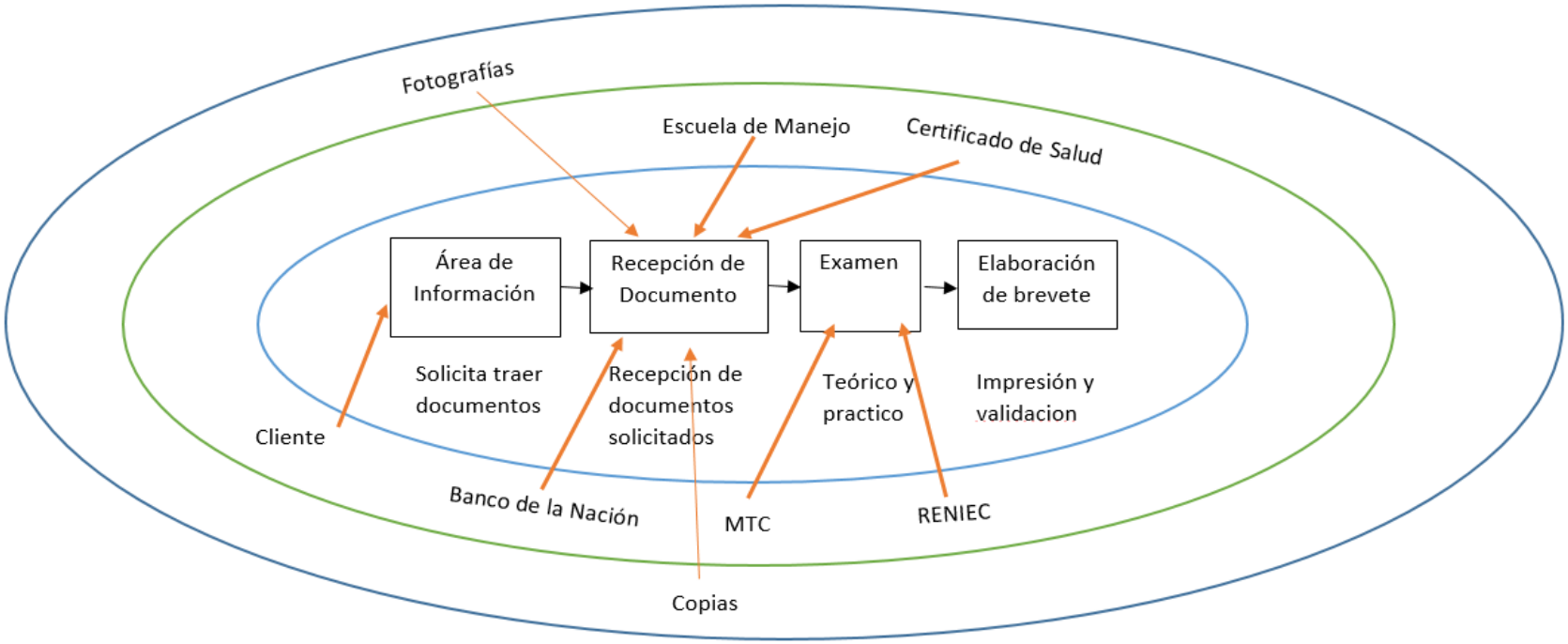
Teniendo en claro la situación real se logró identificar los siguientes requisitos:

1. Determinar el alcance de la seguridad de la información
2. Identificación de los activos de información
3. Clasificar los activos de información
4. Evaluar los activos de información
5. Identificar las vulnerabilidades
6. Identificar la amenaza
7. Hallar el riesgo
8. Determinar las opciones de tratamiento de activos
9. Determinar los controles de acuerdo a la norma ISO/IEC 27001:2014

Una breve descripción con respecto a los requisitos es que primero se definió el alcance que en nuestro caso fue el proceso de emisión de brevetes en la cual se identificó a los activos de información seguidamente se clasifico en términos de hardware, software documentos etc. Seguidamente se evaluó los activos de información en una escala de Likert para el posterior cálculo de riesgo, opción de tratamiento y la declaración de aplicabilidad

4.3 Diagnóstico de la situación actual

GRÁFICO N° 4.2
MÉTODO DE LAS ELIPSES PARA EL PROCESO DE LICENCIAS DE CONDUCIR



Fuente: Elaboración propia.

Para el diagnóstico de la situación actual se usó el método de las elipses para poder describir el proceso de emisión de brevete, en tal sentido la elipse interior muestra los subprocesos que son el área de información, recepción de documento, examen y elaboración de brevete en donde cada uno tiene ciertas tareas como son solicitud de información, recepción de documentos teórico y práctico impresión y validación del brevete.

Bien la elipse interior de los subprocesos interactúa con objetos de la elipse intermedia que son cliente, banco de la nación, Dirección Regional de transporte y comunicación de Áncash, la RENIEC y certificado de salud escuela de manejo.

Por otro lado, la elipse exterior muestra la interacción con la elipse interior que son copias, fotografías.

CAPÍTULO V

DISEÑO DE LA SOLUCIÒN

5.1 Arquitectura tecnológica de la solución

El ciclo de Deming de Edwards Deming, que actualmente conocido como el ciclo de PDCA que son siglas en ingles plan, do, checo y act. Es una mejora continua en el tiempo en donde busca siempre estar en constante mejora de calidad orientada a mejor servicio al cliente. El modelo de Deming es la arquitectura en cual se basa la ISO/IEC 27001:2014 el cual se muestra en el siguiente gráfico.

GRÁFICO N° 5.1

CICLO DE DEMING

Fuente: https://metodoss.com/metodologia-pdca-ciclo-shewhart-deming/.

Para la presente investigación solo se sitúa en el PLAN y teniendo como meta principal elaborar la declaración de aplicabilidad para la entidad de la Dirección Regional de Transporte y Comunicación de Ancash.

GRÁFICO N° 5.2 LA DECLARACIÓN DE APLICABILIDAD ESTÁ DENTRO DE LA FASE DE PLANIFICACIÓN DEL CICLO DE DEMING

Fuente: elaboración propia.

5.2 Diseño de la estructura de la solución

En el presente capitulo se realiza teniendo presente que solo estaremos ubicado en el PLAN de ciclo de Deming y utilizaremos una serie de pasos para gestionar el riesgo.

a) Alcance

El alcance que se identificó está en el método de elipses en donde se detalla el proceso de licencias de conducir de la Dirección Regional de Transporte y

comunicación de Áncash. Con el fin de delimitar nuestra área de trabajo y teniendo en claro que la NTP ISO/IEC 27001:2014 se enfoca en procesos mas no en áreas de oficinas.

b) Identificación de activos de información

Se identificará los activos de información de acuerdo a los procesos concéntricos del método de la elipse.

TABLA N° 5.1

ACTIVOS DE INFORMACIÓN EN EL ÁREA DE INFORMACIÓN

Activo de información	Descripción
Hardware	
Teléfono 1	Básico solo de llamadas
Computadora de escritorio 1	Toshiba I5
Impresora 1	Hp cartucho
Servicios	
Internet	Cableado
Activos de información	
Manual 1	De trámite de brevetes

Fuente: elaboración propia

TABLA N° 5.2

ACTIVOS DE INFORMACIÓN EN EL ÁREA DE RECEPCIÓN DE DOCUMENTO.

Activo de información	Descripción
Hardware	
Teléfono 2	Básico solo de llamadas
Computadora de escritorio 2	Toshiba I5
Impresora 2	Hp cartucho
Servicios	
Internet	Cableado
Activos de información	
Manual de tramites de brevetes	De tramites de brevetes
Documento	
Archivo	Recepción de documento

Fuente: elaboración propia

TABLA N° 5.3

ACTIVOS DE INFORMACIÓN EN EL ÁREA DE INFORMACIÓN EXAMEN

Activos de información	Descripción
Hardware	
Switch	50 puertos para conectar PC
Biométrico	De huella digital
Teléfono 3	Básico solo de llamadas
Computadora de escritorio 3	Toshiba I5
Impresora 3	Hp de cartucho

Servicios	
Internet	
Examen teórico de MTC	En línea dado por MTC
RENIEC	Servicio de identidad
Documento	
Hoja de calificación	es la nota del examen teórico y manejo

Fuente: elaboración propia.

TABLA N° 5.4

ACTIVOS DE INFORMACIÓN EN EL ÁREA DE INFORMACIÓN

ELABORACIÓN DE BREVETE

Activos de información	Descripción
Hardware	
Impresora 4	Hp de cartucho
Computadora escritorio 4	
Lector de código de barras	Motorola para lectura de barras de brevete
Enmicadora	Enmica el brevete
Cortadora	Corta después de enmicar
Teléfono 4	Básico solo llamadas
Servicios	
Registro de código de barras	Registra el brevete por código de barra
Internet	
Documento	
Brevete	Brevete acabado

Fuente: elaboración propia.

c) Tasación de activos de información

Los que evaluaron los activos de información son los mismos propietarios la cual se usó una pregunta que fue ¿Como una falla o perdida en un determinado activo de información afecta la confidencialidad, integridad y disponibilidad? Y para la respuesta se usó la escala de Likert como se muestra en la siguiente tabla.

TABLA N° 5.5

ESCALA PARA CALIFICAR LOS ACTIVOS

Valor cuantitativo	Valor cualitativo
1	Bajo
2	Medio
3	Alto

Fuente: elaboración propia.

Se entiende por los términos de confidencialidad propiedad de que la información no está disponible o divulgada a individuos entidades o procesos no autorizados. Integridad propiedad de salvaguardar la exactitud y la totalidad de los activos. Disponibilidad propiedad de estar accesible y utilizable bajo demanda de una entidad autorizada.

El total se saca la suma entre los valores de los tres campos confidencialidad, integridad y disponibilidad.

TABLA N° 5.6
TASACIÓN DE ACTIVO DE INFORMACIÓN

Activos de Información	Confidencialidad	Integridad	Disponibilidad	Total
Teléfono 1	1	1	1	3
Teléfono 2	1	1	1	3
Teléfono 3	1	1	1	3
Teléfono 4	1	1	1	3
Computadora escritorio 1	1	1	2	4
Computadora escritorio 2	1	1	2	4
Computadora escritorio 3	3	3	3	9
Computadora escritorio 4	3	3	3	9
Impresora 1	1	1	1	3
Impresora 2	1	1	1	3
Impresora 3	3	3	3	9
Impresora 4	3	3	3	9
Internet	3	3	3	9
Manual 1	1	3	1	5
Manual de tramites de brevete	1	2	1	4
Archivo	3	3	3	9
Registro de código de barras	3	3	3	9
Brevete	3	3	3	9
Cortadora	3	2	2	7

Enmicadora	3	3	2	8
Lector de código de barra	3	3	2	8
Hoja de calificación	3	3	3	9
RENIEC	1	3	3	7
Examen teórico de MTC	3	3	3	9
Shitch	3	2	2	7
Biométrico	3	3	3	9

Fuente: elaboración propia.

d) Identificación de vulnerabilidad

Para identificar las vulnerabilidades se utilizó a los trabajadores como fuente de información.

TABLA N° 5.7

IDENTIFICACIÓN DE VULNERABILIDAD PARA CADA ACTIVO DE INFORMACIÓN

ACTIVO	VULNERABILIDAD
Teléfono	fallar el equipo
Computadora escritorio 1	fallar el equipo
Computadora escritorio 2	fallar el equipo
Computadora escritorio 3	fallar el equipo
Computadora escritorio 4	fallar equipo
Impresora 1	fallar el equipo
Impresora 2	fallar el equipo
Impresora 3	fallar el equipo

Impresora 4	fallar el equipo
Internet	sin servicio
Manual 1	pérdida de documento
Manual de tramites de brevete	pérdida de documento
Archivo	pérdida de archivo
Registro de código de barras	fallar el equipo
Brevete	pérdida de documento
Cortadora	falla el equipo
Enmicadora	falla de equipo
Lector de código de barra	fallar el equipo
Hoja de calificación	pérdida documento
RENIEC	sin acceso
Examen teórico de MTC	sin acceso
Shitch	falla el equipo
Biométrico	falla del equipo

Fuente: elaboración propia.

e) Identificación de amenazas

Para identificar las amenazas se cuestionó a los trabajadores como fuente de información.

TABLA N° 5.8

IDENTIFICACIÓN DE AMENAZA PARA CADA VULNERABILIDAD

VULNERABILIDAD	AMENAZA 1	AMENAZA 2
fallar el equipo	mantenimiento	fluido eléctrico
fallar el equipo	mantenimiento	fluido eléctrico
fallar el equipo	Mantenimiento	fluido eléctrico
fallar el equipo	Mantenimiento	fluido eléctrico
fallar equipo	Mantenimiento	fluido eléctrico
fallar el equipo	Mantenimiento	fluido eléctrico
fallar el equipo	Mantenimiento	fluido eléctrico
fallar el equipo	Mantenimiento	fluido eléctrico
fallar el equipo	Mantenimiento	fluido eléctrico
sin servicio	Mantenimiento	fluido eléctrico
pérdida de documento	acceso a terceras personas	
pérdida de documento	acceso a terceras personas	
pérdida de archivo	acceso a terceras personas	
fallar el equipo	Mantenimiento	fluido eléctrico
pérdida de documento	acceso a terceras personas	
falla el equipo	Mantenimiento	
falla de equipo	Mantenimiento	
fallar el equipo	Mantenimiento	flujo eléctrico
pérdida documento	acceso a terceros	
sin acceso	Internet	flujo eléctrico

sin acceso	Internet	flujo eléctrico
falla el equipo	Mantenimiento	flujo eléctrico
falla del equipo	Mantenimiento	flujo eléctrico

Fuente: elaboración propia.

f) Cálculo del riesgo

Para calcular el riesgo primero se tuvo que darles valores a las vulnerabilidades y a sus respectivas amenazas para tal tarea se apoyó a los trabajadores con una escala

TABLA N° 5.9

VALORACIÓN LAS VULNERABILIDADES Y AMENAZAS

Valor cuantitativo	Valor cualitativo	Frecuencia
1	Bajo	1 vez al mes
2	Medio	2 veces al mes
3	Alto	3 veces al mes

Fuente: elaboración propia.

GRÁFICO N° 5.3

CÁLCULO DE RIESGO

	PROPIEDADES					VULNERABILIDAD							RESULTADO	RIESGO	
N°	ACTIVO	C	I	D	TOTAL IMPACTO	VULNERABILIDAD	VALOR	AMENAZA 1	VALOR	AMENAZA 2	VALOR	TOTAL DE AMENAZA	TOTAL DE VUL +AME	CALCULO DE RIESGO	RIESGO
1	Telefono	1	1	1	3	fallar el equipo	1	mantenimiento	1	fluido eléctrico	1	1	2	6	Bajo
2	Computadora escritorio 1	1	1	2	4	fallar el equipo	1	mantenimiento	1	fluido eléctrico	1	1	2	8	Bajo
3	Computadora escritorio 2	1	1	2	4	fallar el equipo	1	mantenimiento	1	fluido eléctrico	1	1	2	8	Bajo
4	Computadora escritorio 3	3	3	3	9	fallar el equipo	1	mantenimiento	1	fluido eléctrico	1	1	2	18	Bajo
5	Computadora escritorio 4	3	3	3	9	fallar equipo	1	mantenimiento	1	fluido eléctrico	1	1	2	18	Bajo
6	Impresora 1	1	1	1	3	fallar el equipo	1	mantenimiento	1	fluido eléctrico	1	1	2	6	Bajo
7	Impresora 2	1	1	1	3	fallar el equipo	1	mantenimiento	1	fluido eléctrico		1	2	6	Bajo
8	Impresora 3	3	3	3	9	fallar el equipo	2	mantenimiento	2	fluido eléctrico	1	1.5	3.5	31.5	Medio
9	Impresora 4	3	3	3	9	fallar el equipo	1	mantenimiento	1	fluido eléctrico	1	1	2	18	Bajo
10	internet	3	3	3	9	sin servicio	1	mantenimiento	1	fluido eléctrico	1	1	2	18	Bajo
11	Manual 1	1	3	1	5	pérdida de documento	1	acceso a terceras personas	1			1	2	10	Bajo
12	Manual de tramites de brevete	1	2	1	4	pérdida de documento	1	acceso a terceras personas	1			1	2	8	Bajo
13	archivo	3	3	3	9	pérdida de archivo	1	acceso a terceras personas	1			1	2	18	Bajo
14	Registro de código de barras	3	3	3	9	fallar el equipo	1	mantenimiento	1	fluido eléctrico	1	1	2	18	Bajo
15	brevete	3	3	3	9	pérdida de documento	1	acceso a terceras personas	1			1	2	18	Bajo
16	Cortadora	3	2	2	7	falla el equipo	1	mantenimiento	1			1	2	14	Bajo
17	Enmicadora	3	3	2	8	falla de equipo	1	mantenimiento	1			1	2	16	Bajo
18	Lector de código de barra	3	3	2	8	fallar el equipo	2	mantenimiento	2	flujo eléctrico	1	1.5	3.5	28	Medio
19	Hoja de calificación	3	3	3	9	pérdida documento	1	acceso a terceros	1			1	2	18	Bajo
20	RENIEC	1	3	3	7	sin acceso	1	Internet	1	flujo eléctrico	1	1	2	14	Bajo
21	Examen teórico de MTC	3	3	3	9	sin acceso	2	Internet	1	flujo eléctrico	1	1	3	27	Medio
22	Shitch	3	2	2	7	falla el equipo	1	mantenimiento	1	flujo eléctrico	1	1	2	14	Bajo
23	biometrico	3	3	3	9	falla del equipo	1	mantenimiento	1	flujo eléctrico	1	1	2	18	Bajo

Fuente: elaboración propia

CAPÍTULO VI

CONSTRUCCIÓN DE LA SOLUCIÓN

6.1 Construcción

6.1.1 Declaración de aplicabilidad

En el capítulo anterior se hizo el diseño de la solución es decir se realizó una serie de pasos para el cálculo del riesgo de cada activo identificado para lo cual se tuvo que identificar los activos, tasarlos, encontrar las amenazas y sus respectivo vulnerabilidades y por último calcular el riesgo de cada activo de información de tal forma usar estrategias para mitigarlas. Ahora la norma técnica peruana ISO/IEC 27001:2014 exige que se desarrolle un documento llamado "la Declaración de aplicabilidad" es en este documento donde se resalta los controles que se deben tener en cuenta para su posterior implementación para mitigar los siniestros de activos de información en la dirección regional de transporte y comunicación de Áncash. El documento debe tener todos los controles que exige la norma técnica peruana ISO/IEC 27001 y se debe justificar el porqué de su posterior implementación y por qué no se debe considerar la cual se encuentra en el anexo A de la norma técnica peruana ISO/IEC 27001:2014. También debe mencionar si se está aplicando o no actualmente el control.

Los formatos que se usó para la elaboración de la declaración de aplicabilidad es la misma que recomienda la norma técnica peruana ISO/IEC 27001 que consta de un cuadro con columnas de cláusulas, sección, objetivo de control aplicabilidad,

control actual y justificación de la exclusión o implementación esto para cada uno de los controles.

El documento de declaración de aplicabilidad se presenta en el contexto de la dirección Regional de Transporte y Comunicación de Ancash en la subdirección de licencias de conducir específicamente en el proceso de emisión de brevete este documento se encuentra en el anexo como producto final de la presente investigación.

La declaración de aplicabilidad se encuentra en el plan del ciclo de Deming para su posterior implementación que se situara en el hacer todo ello en el progreso de la mejora continua.

CAPÍTULO VII

IMPLEMENTACIÓN

7.1 Monitoreo y evaluación de la solución

7.1.1 Plan de monitoreo y evaluación

En un contexto ideal en donde, con la venia de los altos directivos y con un presupuesto aprobado para la implementación de controles se podría hablar de monitoreo y evaluación sin embargo es una de las limitantes para la presente investigación por tanto se propondrá una metodología para el monitoreo y evaluación que es el siguiente.

Se propone usar la metodología del ciclo de Deming de Edwards Deming también conocido como el ciclo PDCA que significa planificar hacer verificar hacer este método es muy bueno para mejorar los sistemas de gestión para lo cual se necesita un tiempo de 6 meses mínimo para poder evaluar y así mejorar la cual consiste en los siguiente:

Plan; es la planificación de las acciones que se debería realizar, los controles que deberían implementares y las políticas que debería seguirse en este punto se centró la presente tesis que fueron; la identificación de activos, la evaluación de los activos, identificación de amenazas, vulnerabilidades, el cálculo de riesgo y la propuesta de la declaración de aplicabilidad para la dirección regional de transporte y comunicación de Áncash.

Hacer; todo lo dicho en el plan debe implementarse tal cual.

Verificar; se debe tomar apuntes sobre las anomalías, eventos no deseado y desastres detectado

Hacer; una vez evaluado se toma correcciones para mejorar y seguir con el círculo de Deming para seguir mejorando

7.1.2 Bitácora y puesta a punto

En el presente proyecto se realizó apuntes sobre el desarrollo de la investigación la cual se empleó la siguiente tabla

TABLA N° 7.1
BITÁCORA PARA EL DESARROLLO DE PROYECTO

Fecha	Etapa	Actividad	Observación
Del 03/03/2018 al 01/04/2018	Análisis	Recopilar información	Se realizó sin inconveniente
		Analizar información	Se realizó sin inconveniente
Del 02/04/2018 al 01/07/2018	Diseño	Calculo de riesgo	Se realizó sin inconveniente
		Proponer controles	Se realizó sin inconveniente
	Construcción	Establecer la declaración de aplicabilidad	Se realizó sin inconveniente

Fuente: elaboración propia.

CAPÍTULO VIII

RESULTADOS

Resultado según el objetivo general: Conocer cómo la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 mitigara los siniestros de los activos de información en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash.

GRÁFICO N° 8.1

RELACIÓN DE SPEARMAN

			VAR00001	VAR00002
Rho de Spearman	VAR00001	Coeficiente de correlación	1,000	,782**
		Sig. (bilateral)	.	,000
		N	108	108
	VAR00002	Coeficiente de correlación	,782**	1,000
		Sig. (bilateral)	,000	.
		N	108	108

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

Fuente: elaboración propia.

El coeficiente de correlación de Spearman se encuentra en un intervalo de -1 1, para este caso es de 0.782 que indica un grado de relación alto y es proporcional entre la variable declaración de aplicabilidad y siniestros de información. El nivel de significancia fue 0.01 que es en un 99% confianza en que la relación es verdadera.

Resultado según el objetivo específico: Establecer de qué manera la declaración de aplicabilidad mitigara el daño de los siniestros de la información mediante el contexto

de la organización de la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash.

GRÁFICO N° 8.2

RELACIÓN DE SPEARMAN

			VAR00001	VAR00002
Rho de Spearman	VAR00001	Coeficiente de correlación	1,000	,562
		Sig. (bilateral)		,000
		N	108	108
	VAR00002	Coeficiente de correlación	,562	1,000
		Sig. (bilateral)	,000	
		N	108	108

Fuente: elaboración propia

El coeficiente de correlación de Spearman se encuentra en un intervalo de -1 1, para este caso es de 0.562 que indica un grado de relación alto y es proporcional entre la variable declaración de aplicabilidad y contexto de la organización.

Resultado según el objetivo específico: Establecer de qué manera la declaración de aplicabilidad mitigara el daño de los siniestros de la información mediante la planificación de la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash

GRÁFICO N° 8.3

RELACIÓN DE SPEARMAN

			VAR00001	VAR00002
Rho de Spearman	VAR00001	Coeficiente de correlación	1,000	,769
		Sig. (bilateral)		,000
		N	108	108
	VAR00002	Coeficiente de correlación	,769	1,000
		Sig. (bilateral)	,000	
		N	108	108

Fuente: elaboración propia.

El coeficiente de correlación de Spearman se encuentra en un intervalo de -1 1, para este caso es de 0.769 que indica un grado de relación alto y es proporcional entre la variable declaración de aplicabilidad y planificación de la NTP-ISO/IEC 27001:2014.

Resultado según el objetivo específico: Elaborar la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash.

La declaración de aplicabilidad (ver anexo de declaración de aplicabilidad) es un documento la cual muestra los 133 controles (medidas de seguridad) sugeridos en el Anexo A de la norma ISO 27001 que consta de un cuadro con columnas de cláusulas, sección, objetivo de control aplicabilidad, control actual y justificación de la exclusión o implementación esto para cada uno de los controles en el contexto de la dirección Regional de Transporte y Comunicación de Ancash.

CAPÍTULO IX

DISCUSIÓN DE RESUTADOS

Según el objetivo general Conocer cómo la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 mitigara los siniestros de los activos de información en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash, Los resultados obtenidos en el grafico N° 8.1 se evidencia la relación de forma proporcional ρ=0.782** entre las variables declaración de aplicabilidad y siniestros de la información datos al ser comparados con lo encontrado por Aranda (2009) en su tesis "Implementación del primer sistema de gestión de seguridad de la información, en el ecuador, certificado bajo la norma ISO 27001:2005 " que concluyo que tener implementado un sistema de gestión de seguridad de la información no significa contar con una seguridad máxima sino que se reduce los riesgos de forma paulatina porque mejora cada vez que de la vuelta el ciclo de Deming, con estos resultados se afirma que la declaración de aplicabilidad mitigara los siniestros de información en la en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash, además (NTP-ISO/IEC 27001,2014) indica que la Declaración de aplicabilidad es el nexo principal entre la evaluación y el tratamiento del riesgo y la implementación de su sistema de seguridad de la información. El objetivo de este documento es definir cuáles de los 133 controles (medidas de seguridad) sugeridos en el Anexo A de la norma ISO 27001 son los que se implementará y posterior ayudará a minimizar los siniestros de la información.

Según el objetivo específico Establecer de qué manera la declaración de aplicabilidad mitigara el daño de los siniestros de la información mediante el contexto de la organización de la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash, Los resultados obtenidos en el grafico N° 8.2 se evidencia la relación de forma proporcional ρ=0.562 entre las variables declaración de aplicabilidad y contexto de la organización datos que al ser comparados con lo encontrado por Romero (2006) en su tesis Plan de Seguridad Informática en el MTC, que concluye que, las organizaciones tanto externo como interno deben tratar de hacer lo más llevadero posible las tareas operativas del sistema SGSI, en beneficio de las partes interesadas, para lo cual necesitan la ayuda de herramientas tecnológicas que automaticen ciertas tareas. con estos resultados se afirma que la declaración de aplicabilidad mitigara los siniestros de información mediante el contexto de la organización en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash. además (NTP-ISO/IEC 27001,2014) indica que el contexto de la organización, lo Primero son los aspectos externos e internos referidos a comprender la organización y su contexto, segundo los requisitos referidos a comprender las necesidades y expectativas de las partes interesadas y por último identificar las interfaces y dependencias entre actividades realizadas por la organización y las que son realizadas por otras organizaciones.

Según el objetivo específico establecer de qué manera la declaración de aplicabilidad mitigara el daño de los siniestros de la información mediante la planificación de la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash. Los resultados obtenidos en el grafico N° 8.3 se evidencia la relación de forma proporcional ρ=0.769 entre las variables declaración de aplicabilidad y Planificación de la NTP-ISO/IEC 27001 datos que al ser comparados con lo encontrado por Aguirre (2014) es su tesis Diseño de un Sistema de Gestión de Seguridad de la Información para Servicios Postales del Perú, concluyo que es necesario mejorar la comunicación con el área de logística para acelerar los procesos de compra de aquellos activos que nos ayudaran en el tratamiento de riesgos detectados, especialmente, si estos riesgos son considerados alto o graves en la organización. con estos resultados se afirma que la declaración de aplicabilidad mitigara los siniestros de información mediante la planificación de la NTP-ISO/IEC 27001 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash. además, la NTP-ISO/IEC 27001,2014) en la cual dice que hay que considerar los asuntos referido al contexto de la organización, determinar los riesgos y oportunidades que necesitan ser tratados para asegurar que el sistema de gestión de seguridad de la información pueda lograr su resultado esperado y lograr la mejora continua.

Según el objetivo específico Elaborar la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash. Los resultados obtenidos (ver anexo de declaración de aplicabilidad) muestra los controles que son medidas de seguridad que se debería implementarse al ser comparado con lo encontrado por Buenaño y Granda (2009) en su tesis Planeación y diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001-27002 que tuvo como conclusión que la norma ISO 27001 está orientada al tratamiento de la seguridad de la información mediante la gestión de riesgo que luego recae en la declaración de aplicabilidad, tanto para sus activos como para sus proceso, esto garantiza que ante recursos limitados las inversiones sean bien focalizados con estos resultados se afirma que la declaración de aplicabilidad es un documento que detalla los controles a implementarse para mejorar la seguridad de la información, además la (NTP-ISO/IEC 27001,2014) indica que la Declaración de aplicabilidad es el nexo principal entre la evaluación y el tratamiento del riesgo y la implementación de su sistema de seguridad de la información. El objetivo de este documento es definir cuáles de los 133 controles (medidas de seguridad) sugeridos en el Anexo A de la norma ISO 27001 son los que se implementará y posterior ayudará a minimizar los siniestros de la información.

CONCLUSIONES

Luego de haber realizado la presente investigación se concluyó lo siguiente:

- Existe relación significativa (ρ=0.782, sig. 0.001) entre declaración de aplicabilidad y siniestros de la información en la DRTCA, 2018, afirmando que la declaración de aplicabilidad mitigara los siniestros de información en la en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash, por otro lado, se realizó la prueba de hipótesis obteniendo como resultado la aceptación de la hipótesis de investigación y rechazando la hipótesis nula.
- Existe relación (ρ=0.562) entre declaración de aplicabilidad y contexto de la organización, afirmando que la declaración de aplicabilidad mitigara los siniestros de información mediante el contexto de la organización en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash.
- Existe relación (ρ=0.769) entre declaración de aplicabilidad y planificación, afirmando que la declaración de aplicabilidad mitigara los siniestros de información mediante la planificación de la NTP-ISO/IEC 27001 en DRTCA.
- La declaración de aplicabilidad es un documento que contiene los controles a implementar con la cual se evidencia una clara necesidad de personas especializadas para poder implementar los controles de seguridad de información que se señaló en la declaración de aplicabilidad.

RECOMENDACIONES

- A la gerencia de la sub dirección de licencias de conducir implantar la declaración de aplicabilidad para seguir mejorando a la seguridad de la información.
- A los trabajadores de la dirección de licencias de conducir conocer sus contexto interno y externo en cuanto a las vulnerabilidades y amenazas.
- Al proceso de emisión de brevete de la dirección de licencias de conducir planificar la evaluación de activos de información cada 6 meses.
- La entidad debe poner en sus objetivos la seguridad de la información así tenga más importancia la declaración de aplicabilidad para su posterior implementación.

REFERENCIA BIBLIOGRAFICA

Alexander G., Alberto. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información; Óptica ISO/ IEC 27001:2005*. Bogotá: Alfaomega Colombiana S.A.

Aguirre, D. (2014*). Diseño de un Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A.* (Tesis de Grado). Pontificia Universidad Católica, Lima, Perú.

Ángeles, S. (2008). *Sistema de gestión de seguridad de información ISO 27001 para un Data Center* (Tesis de grado). Universidad Nacional de Ingeniería, Lima, Perú.

Aranda, J. (2009). *Implementación del primer sistema de gestión de seguridad de la información en el ecuador certificado bajo la norma ISO 27001:2005* (Tesis de grado). Escuela Superior Politécnica del Litoral, Guayaquil, Ecuador.

Buenaño,J y Granda, M (2009). *Planeación y diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001-27002. Guayaquil, Ecuador*. (Tesis de grado). Universidad Politécnica Salesiana. Obtenido de: http://dspace.ups.edu.ec/bitstream/123456789/3178/1/UPS-GT000102.pdf

Carrasco, S. (2013). *Metodología de la investigación científica* (6 ed.). Lima: San Marcos.

Hernández, R. (2014). *Metodología de la investigación* (6 ed.). Mexico, D. F.: McGRAW-HILL.

Mory, A. (2014). *Aplicación de la norma ISO/IEC 27001 para mejorar la seguridad de la información en la empresa HM Contratistas S.A.* (Tesis de grado). Universidad Nacional Santiago Antúnez de Mayolo, Ancash, Perú.

Merino Bada, C. y Cañizares Sales, R. (2011). Implantación de un sistema de gestión de seguridad de la información según ISO 27001. Madrid: Fundación Confemetal.

Oficina nacional de gobierno electrónico e informática. (08 de Enero de 2016). *Aprobacion de la NTP-ISO/IEC 27001*. Lima. Obtenido de http://busquedas.elperuano.pe/normaslegales/aprueban-el-uso-obligatorio-de-la-norma-tecnica-peruana-ntp-resolucion-ministerial-no-004-2016-pcm-1333015-1/

Romero, V. (2006). *Plan de Seguridad Informática en el MTC (tesis de grado)*. Universidad Nacional de Ingeniería, Lima, Perú.

Tomayo, M. (2003). *El proceso de la investigación cientifica* (4 ed.). Mexico D. F.: Limusa.

ANEXOS

A) ANEXO DE FIGURAS

Figura 1. Personas encuestadas

Figura 2. Área del trámite de licencias de conducir

Figura 3. Ventanilla de mesa de partes

Figura 4. Trabajador del proceso de licencias de conducir

Figura 5. El trabajador cuya función es permitir el paso al interior de la entidad

Figura 6. El área interior de la entidad

Figura 7. Área de examen teórico para la obtención de brevete

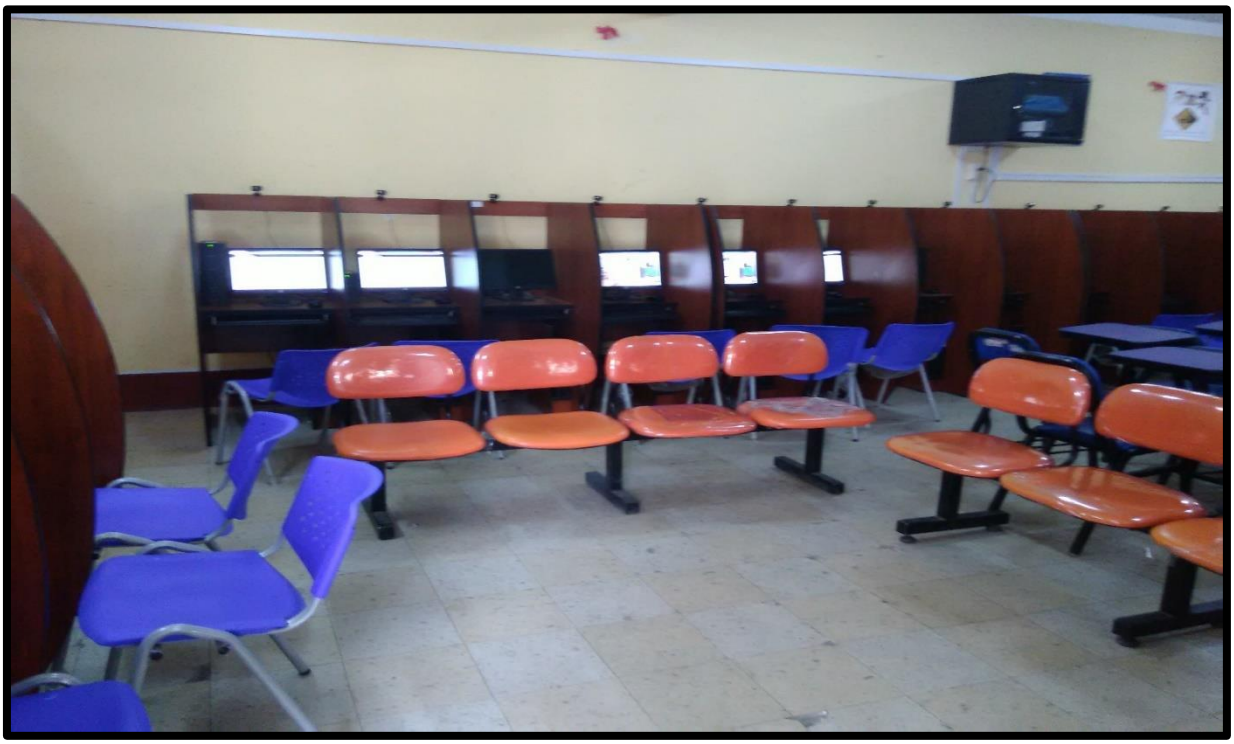


Figura 8: Trabajador encargado del área del examen teórico

Figura 9. Sensor de huella digital para poder dar el examen teórico

Figura 10. Documento de resultados de evaluación de examen teórico y practico

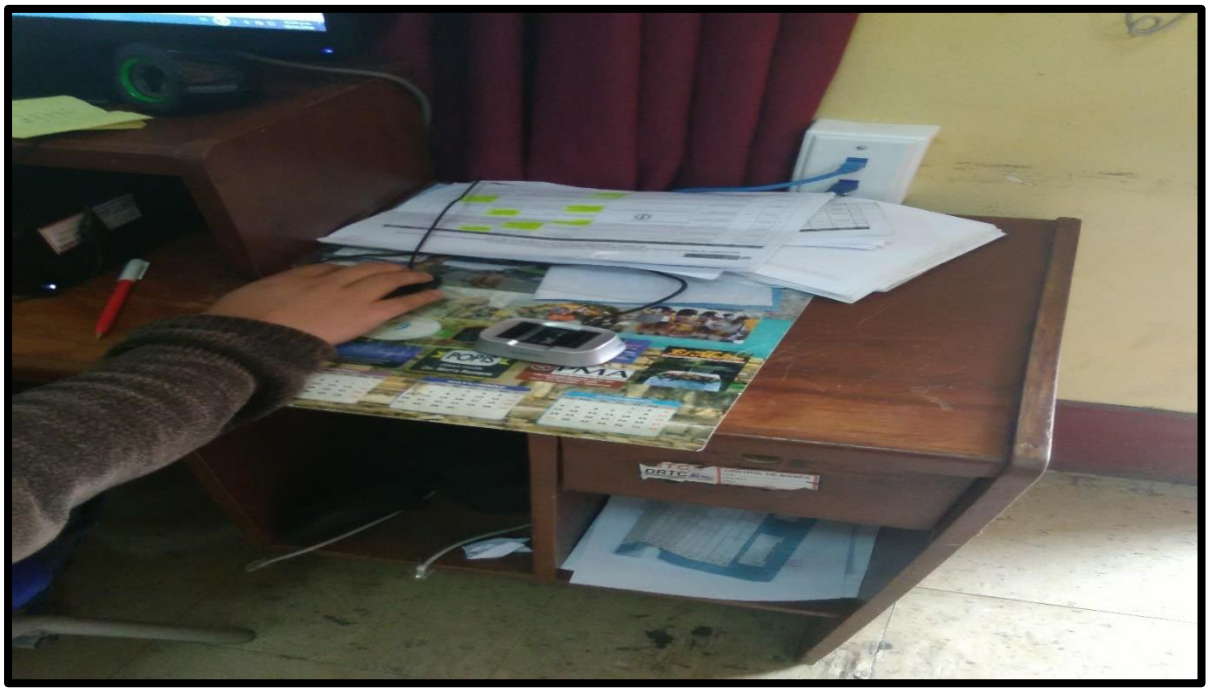


Figura 11. Área de impresión de brevetes

Figura 12. Equipos en el área de brevetes

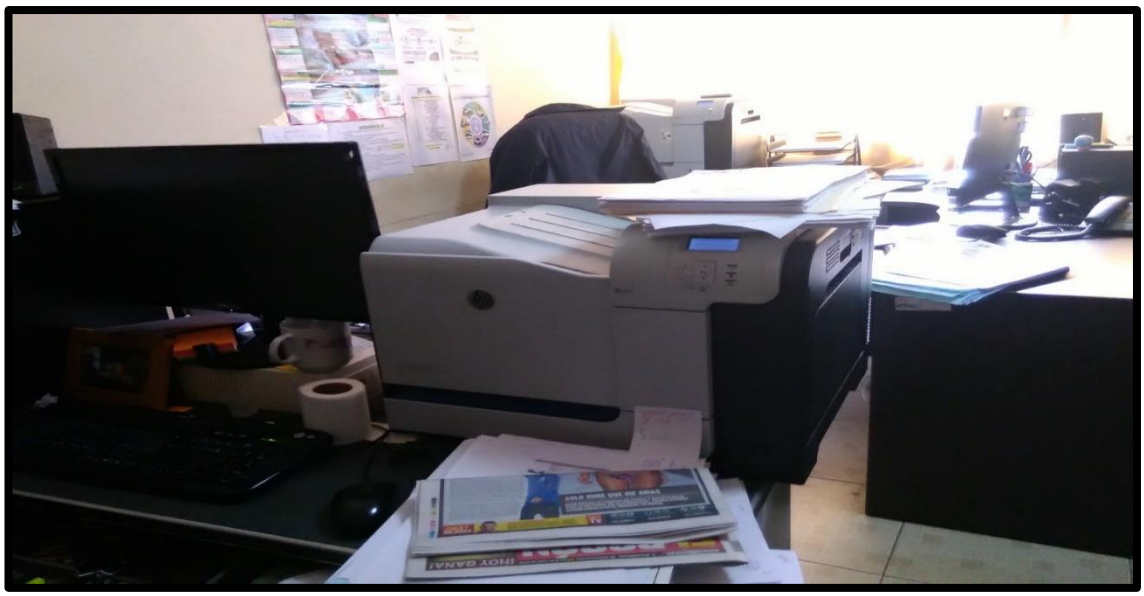


Figura 13. Equipos para elaboración del brevete enmicadora y colocación de

Figura 14. Impresión de brevetes.

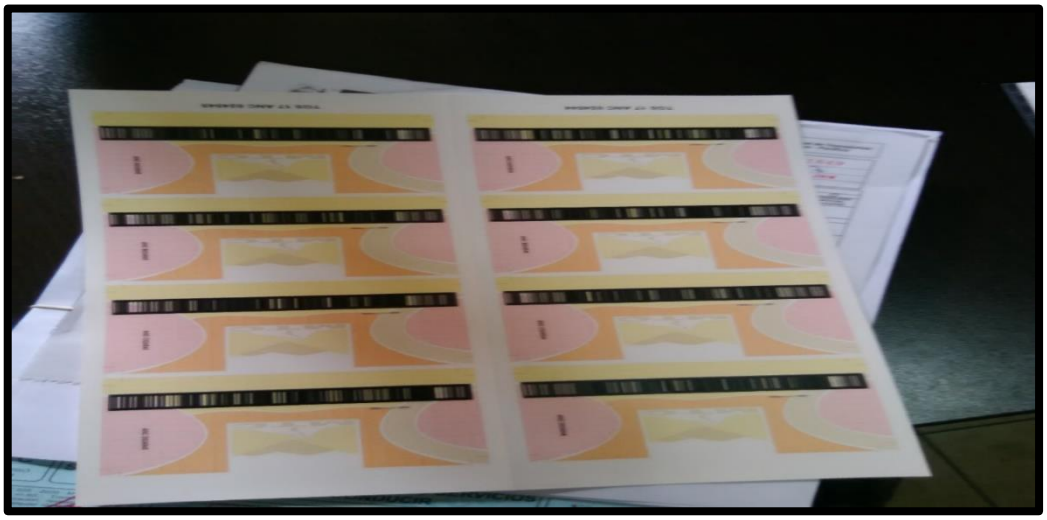


Figura 15. Registro por código de barra del brevete

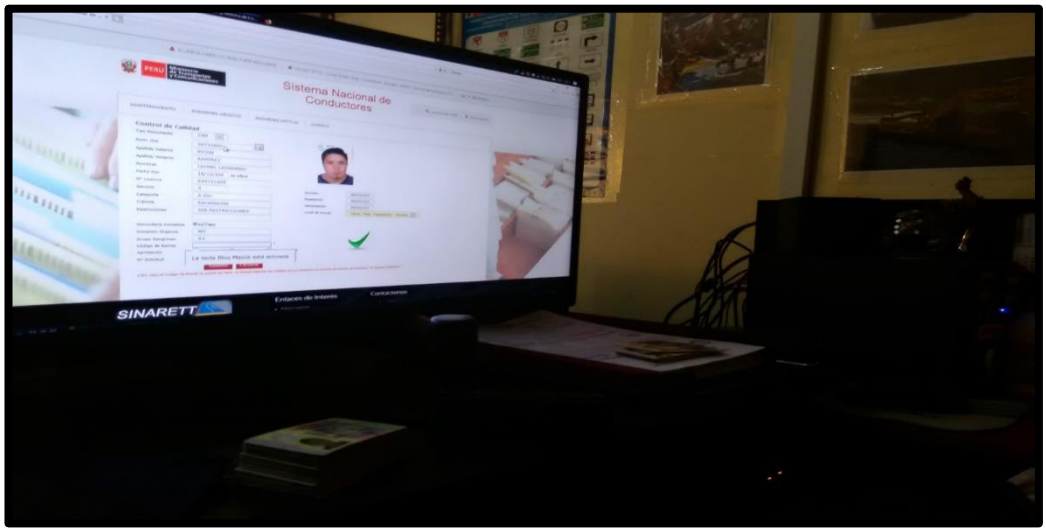
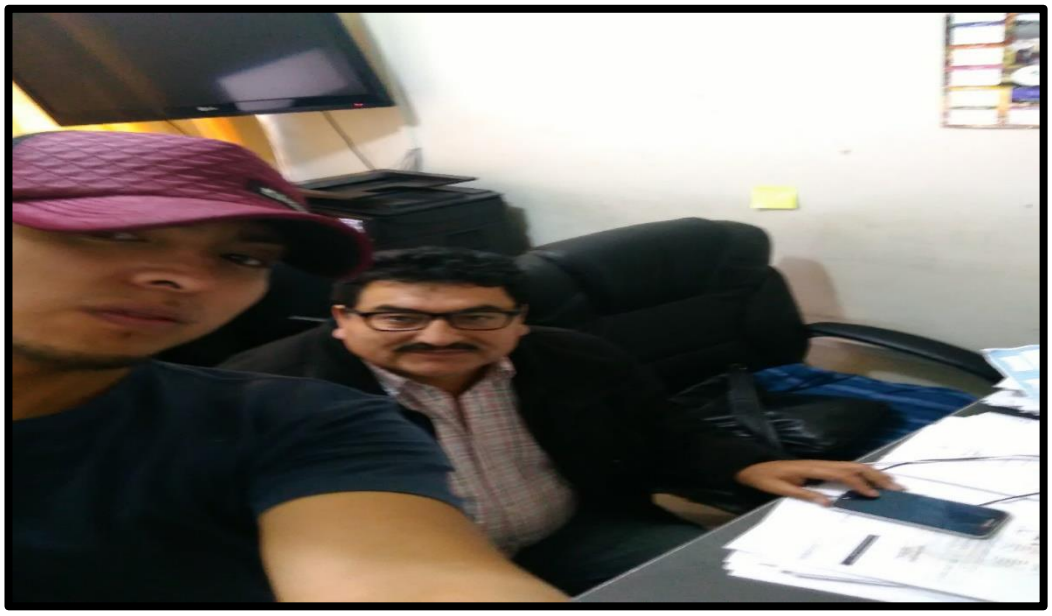


Figura 16. El jefe de la subgerencia de brevetes



Anexo: Operacionalización de variables

VARIABLES	DEFINICION CONCEPTUAL	DEFINICION OPERACIONAL	DIMENSIONES	INDICADORES
VARIABLE INDEPENDIENTE Declaración de aplicabilidad	Es un documento que en lista los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001 (un conjunto de 114 controles agrupados en 35 objetivos de control.	A partir de la información que se obtenga de la DRTCA se usara un modelo de planificación de riesgo para obtener procesar información	Controles	Físico
				software
VARIABLE INTERMEDIA NTP-ISO/IEC 27001:2014	La NTP ISO/IEC 27001:2014 está compuesta por 10 ítems de las cuales se considera como fundamental o es la piedra angular del sistema de gestión de seguridad de la información; el contexto de la organización, evaluación y tratamiento de la información en suma los ítems está diseñado para proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI. (ISO/IEC 27001, 2014)	A partir de seguir un modelo se obtendrá información que facilitara la planificación de riesgo	Contexto de la organización	Interno
				externo
			Planificación	Evaluación
				tratamiento
VARIABLE DEPENDIENTE Siniestros de los activos de información	Suceso que produce un daño a los activos de información (RAE, 2018)	Se analizara y procesara información sobre los siniestros a partir de un modelo de planificación de riesgo	Daño	Perdida de dinero
				Perdida de imagen

Anexo: matriz de consistencia

PROBLEMA		HIPÓTESIS		OBJETIVO	
General	**Específicos**	**General**	**Específicos**	**General**	**Específicos**
¿Cómo la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 mitigara los siniestros de los activos de información en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash?	P1: ¿De qué manera la declaración de aplicabilidad mitigara el daño de los siniestros de la información mediante el contexto de la organización de la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash? P2: ¿De qué manera la declaración de aplicabilidad mitigara el daño de los siniestros de la información mediante la planificación de la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash?	Con la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 se mitigara los siniestros de los activos de información en la subdirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash.	H1: Con la declaración de aplicabilidad se mitigara el daño de los siniestros de la información mediante el contexto de la organización de la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash. H2: Con la declaración de aplicabilidad se mitigara el daño de los siniestros de la información mediante planificación de la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash.	Conocer cómo la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 mitigara los siniestros de los activos de información en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash.	O1. Establecer de qué manera la declaración de aplicabilidad mitigara el daño de los siniestros de la información mediante el contexto de la organización de la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash. O2. Establecer de qué manera la declaración de aplicabilidad mitigara el daño de los siniestros de la información mediante la planificación de la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash.

ANEXO DE ENCUESTA

ENCUESTA DE OPINIÓN DEL PROCESO DE LICENCIA DE CONDUCIR PARA LA SEGURIDAD DE LA INFORMACIÓN DE LA SUBGERENCIA DE LICENCIAS DE CONDUCIR DE LA DRTCA

INDICACIONES:

Estimado colaborador: agradezco de antemano su aporte en la presente investigación, sírvase responder la siguiente escala de valoración de manera sincera y objetiva respecto al proceso de licencias de conducir de la subgerencia de licencias de conducir. Cabe mencionar, que este proceso va en constante mejora continua con uso intensivo de las Tecnologías de la Información. Marque con una (x) en la alternativa que se adapte mejor a su opinión:

ESCALA DE VALORACION	VALOR
Malo	1
Regular	2
Bueno	3

DIMENSIONES	Nº	INDICADORES	CRITERIOS	(1)	(2)	(3)
Controles de la seguridad	1	Físico	1. ¿Cómo valora usted la seguridad de su trámite de licencia de conducir en términos de equipos? ej. Cámaras de vigilancia, huella digital			
	2	Hardware	2. ¿Cómo valora usted la seguridad de su trámite de licencia de conducir en términos de programas? ej. Antivirus			
Contexto de la organización	3	Interno	3. ¿Cómo valora usted el trabajo del personal interno en el trámite de licencias de conducir?			
	4	Externo	4. ¿Cómo valora usted el trabajo del personal externo en el trámite de licencias de conducir? ej. Escuelas de manejo			
Planificación	5	Evaluación	5. ¿cómo valora usted el trabajo del personal para identificar los riesgos que se puedan dar en la perdida la información en el trámite de licencias de conducir?			
	6	tratamiento	6. ¿cómo valora usted el trabajo del personal para evitar que se pierda la información en el trámite de licencias de conducir?			
Daño	7	dinero	7. ¿cómo valora usted el trabajo que se hace para evitar pérdida de información en esta oficina?			
	8	imagen	8. ¿cómo valora usted el trabajo que se hace para evitar la perdía de imagen de la DRTCA?			

ANEXO DE ESTADISTICA

Escala: ALL VARIABLES

Resumen de procesamiento de casos

		N	%
Casos	Válido	20	100,0
	Excluido[a]	0	,0
	Total	20	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,847	8

Estadísticas de total de elemento

	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
VAR00001	15,1000	10,726	,510	,847
VAR00002	14,6000	8,568	,731	,810
VAR00003	14,2000	9,958	,429	,845
VAR00004	14,9000	7,568	,829	,792
VAR00005	14,9500	7,418	,918	,778
VAR00006	14,8000	7,432	,726	,811
VAR00007	15,0500	11,524	,000	,864
VAR00008	15,7500	8,934	,469	,847

Figura 1. Prueba de alfa de Cronbach

ANEXO DE LA BASE DE DATO

BASE DE DATO														
X: DECLARACION DE APLICABILIDAD											Y: SINIESTROS EN LA INFORMACION			
N°	X1: CONTROL DE SEGURIDAD			X2: CONTEXTO DE LA ORGANIZACIÓN			X3: PLANIFICACION				Y1: DAÑO			
	1	2	SUB	1	2	SUB	1	2	SUB	TOTAL	1	2	SUB	TOTAL
1	3	3	6	3	3	6	3	3	6	18	3	3	6	6
2	3	3	6	3	3	6	3	3	6	18	3	3	6	6
3	3	3	6	3	3	6	3	3	6	18	3	3	6	6
4	1	1	2	1	1	2	1	1	2	6	1	1	2	2
5	3	3	6	3	3	6	3	3	6	18	3	3	6	6
6	3	3	6	3	3	6	3	3	6	18	3	3	6	6
7	3	2	5	3	1	4	2	2	4	13	3	3	6	6
8	2	2	4	2	2	4	2	2	4	12	2	2	4	4
9	3	3	6	3	3	6	3	3	6	18	3	3	6	6
10	3	3	6	3	3	6	3	3	6	18	3	3	6	6
11	3	3	6	3	3	6	3	3	6	18	3	3	6	6
12	2	2	4	2	2	4	2	2	4	12	2	2	4	4
13	3	3	6	3	3	6	3	3	6	18	3	3	6	6
14	3	3	6	3	3	6	3	3	6	18	3	3	6	6
15	3	3	6	3	3	6	3	3	6	18	3	3	6	6
16	3	3	6	3	3	6	3	3	6	18	3	3	6	6
17	3	3	6	3	3	6	3	3	6	18	3	3	6	6
18	3	3	6	3	3	6	3	3	6	18	3	3	6	6
19	2	2	4	2	2	4	2	2	4	12	2	2	4	4
20	3	3	6	3	3	6	3	3	6	18	3	3	6	6
21	3	3	6	3	3	6	3	3	6	18	3	3	6	6
22	3	3	6	3	3	6	3	3	6	18	3	3	6	6
23	3	3	6	3	3	6	3	3	6	18	3	3	6	6
24	3	3	6	3	3	6	3	3	6	18	3	3	6	6
25	3	3	6	3	3	6	3	3	6	18	3	3	6	6
26	2	2	4	2	2	4	2	2	4	12	2	2	4	4
27	3	3	6	3	3	6	3	3	6	18	3	3	6	6
28	3	3	6	3	3	6	3	3	6	18	3	3	6	6

29	3	3	6	3	3	6	3	3	6	18	3	3	6	6
30	3	3	6	1	3	4	1	1	2	12	1	1	2	2
31	3	3	6	3	3	6	3	3	6	18	3	3	6	6
32	3	1	4	2	2	4	1	2	3	11	1	2	3	3
33	3	3	6	3	3	6	3	3	6	18	3	3	6	6
34	3	2	5	2	3	5	2	2	4	14	3	2	5	5
35	3	2	5	2	3	5	3	2	5	15	2	2	4	4
36	3	2	5	2	3	5	2	2	4	14	2	1	3	3
37	3	3	6	3	3	6	3	3	6	18	3	3	6	6
38	2	3	5	2	2	4	1	2	3	12	1	2	3	3
39	3	2	5	2	3	5	2	2	4	14	2	2	4	4
40	3	3	6	3	3	6	3	3	6	18	3	3	6	6
41	3	3	6	3	3	6	3	3	6	18	3	3	6	6
42	3	2	5	2	2	4	2	1	3	12	3	3	6	6
43	3	2	5	2	3	5	2	2	4	14	2	2	4	4
44	2	2	4	2	2	4	1	2	3	11	3	2	5	5
45	3	2	5	3	3	6	2	2	4	15	3	3	6	6
46	3	2	5	2	3	5	2	2	4	14	1	2	3	3
47	3	2	5	2	2	4	2	2	4	13	3	2	5	5
48	3	2	5	2	3	5	2	2	4	14	3	2	5	5
49	3	2	5	2	3	5	2	2	4	14	2	3	5	5
50	2	1	3	2	3	5	3	2	5	13	3	2	5	5
51	3	3	6	3	3	6	2	3	3	15	3	2	5	5
52	3	2	5	2	1	3	1	2	3	11	2	2	4	4
53	2	2	4	2	2	4	2	2	4	12	2	2	4	4
54	2	2	4	2	2	4	2	2	4	12	2	2	4	4
55	3	2	5	2	3	5	2	2	4	14	2	1	3	3
56	2	2	4	2	3	5	2	2	4	13	3	2	5	5
57	3	2	5	3	3	6	2	2	4	15	3	2	5	5
58	3	1	4	2	2	4	2	2	4	12	2	2	4	4
59	3	2	5	2	3	5	2	1	3	13	1	2	3	3
60	3	2	5	2	3	5	3	2	5	15	2	2	4	4
61	3	2	5	2	3	5	2	2	4	14	3	3	6	6

62	3	2	5	2	3	5	2	2	4	14	2	2	4	4
63	2	2	4	2	3	5	2	3	5	14	3	3	6	6
64	3	2	5	1	2	3	2	2	4	12	1	2	3	3
65	3	3	6	3	3	6	3	3	6	18	3	3	6	6
66	3	2	5	2	1	3	2	2	4	12	3	2	5	5
67	3	2	5	2	3	5	2	2	4	14	3	2	5	5
68	2	1	3	2	3	5	2	2	4	12	2	1	3	3
69	3	2	5	2	2	4	3	1	4	13	3	3	6	6
70	3	2	5	2	3	5	2	2	4	14	1	2	3	3
71	3	2	5	2	3	5	2	2	4	14	2	2	4	4
72	3	2	5	2	3	5	2	2	4	14	3	2	5	5
73	3	2	5	2	3	5	2	2	4	14	3	1	4	4
74	2	2	4	3	3	6	1	2	3	13	2	2	4	4
75	3	2	5	2	2	4	3	2	5	14	1	2	3	3
76	3	2	5	2	3	5	2	2	4	14	2	3	5	5
77	3	2	5	2	3	5	2	2	4	14	3	2	5	5
78	3	2	5	2	1	3	2	2	4	12	2	2	4	4
79	3	3	6	3	3	6	3	3	6	18	3	3	6	6
80	3	2	5	2	3	5	2	2	4	14	3	2	5	5
81	3	2	5	2	2	4	2	1	3	12	2	2	4	4
82	3	3	6	3	3	6	3	3	6	18	3	3	6	6
83	2	2	4	2	2	4	2	2	4	12	2	2	4	4
84	2	2	4	2	2	4	2	2	4	12	2	2	4	4
85	3	3	6	3	3	6	3	3	6	18	3	3	6	6
86	3	3	6	3	3	6	3	3	6	18	3	3	6	6
87	3	3	6	3	3	6	3	3	6	18	3	3	6	6
88	3	3	6	3	3	6	3	3	6	18	3	3	6	6
89	2	2	4	2	3	5	2	2	4	13	2	3	5	5
90	3	2	5	2	3	5	2	2	4	14	3	2	5	5
91	3	2	5	2	3	5	2	2	4	14	3	2	5	5
92	3	3	6	3	3	6	3	3	6	18	3	3	6	6
93	3	1	4	2	3	5	2	2	4	13	3	3	6	6
94	3	2	5	3	2	5	2	2	4	14	3	2	5	5

95	2	2	4	2	1	3	2	2	4	11	2	2	4	4
96	3	2	5	2	3	5	3	2	5	15	3	2	5	5
97	3	3	6	3	3	6	3	3	6	18	3	3	6	6
98	3	3	6	3	3	6	3	3	6	18	3	3	6	6
99	3	3	6	3	3	6	3	3	6	18	3	3	6	6
100	3	3	6	3	3	6	3	3	6	18	3	3	6	6
101	2	2	4	2	3	5	2	2	4	13	2	2	4	4
102	3	2	5	2	3	5	2	2	4	14	3	2	5	5
103	3	3	6	3	3	6	3	3	6	18	3	3	6	6
104	3	3	6	3	3	6	3	3	6	18	3	3	6	6
105	3	2	5	2	3	5	3	3	6	16	1	2	3	3
106	3	1	4	2	3	5	2	2	4	13	3	1	4	4
107	2	2	4	1	3	4	2	2	4	12	2	2	4	4
108	3	3	6	3	3	6	3	3	6	18	3	3	6	6

Figura 1. Base de dato de las encuestas realizadas

ANEXO DE DECLARACION DE APLICABILIDAD

DECLARACION DE APLICABILIDAD

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
5. políticas de seguridad	5.1	Dirección de la alta gerencia para la seguridad de la información			
	5.1.1	Política de seguridad de la información	Si		Es necesario establecer políticas de seguridad de información para estar claros en el resguardo de los activos de información
	5.1.2	Revisión de las políticas de seguridad de la información	Si		Se debe evaluar el documento de políticas de seguridad cada cierto tiempo

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
6. organización de la seguridad de la información	6.1	Organización interna			
	6.1.1	Roles y responsabilidades para la seguridad de la información	No	Existe un documento en donde se detalla los roles y responsabilidades de los trabajadores	Al existir se excluye este control
	6.1.2	Segregación de funciones	No	Existe un organigrama de funciones de fácil entendimiento	Al existir se excluye el control
	6.1.3	Contacto con autoridades	Si		Identificar a las autoridades pertinentes quienes ayudaran a fortalecer la seguridad de la información
	6.1.4	Contacto con grupo de interés especial	Si		La entidad debe identificar los principales grupos de interés como son la RENIEC, MTC para poder identificar las posibles vulnerabilidades y estar preparados ante cualesquiera amenazas

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
6. organización de la seguridad de la información	6.1.5	Seguridad de la información en gerencia de proyecto	Si		El presente proyecto debe alinearse con la gestión de proyectos teniendo en cuenta que la DRTCA salvaguarde sus intereses en cuanto la seguridad de la información por tanto se hablaría de un sistema gestión integral.
	6.2	Dispositivo móviles y teletrabajo			
	6.2.1	Política en dispositivo móviles	No	No se considera ya que la entidad no usa celulares como medio de trabajo todo se hace por otro medio	Al no tener presente este tipo de activo se excluye el control
	6.2.2	teletrabajo	No	No se considera ya que la entidad no usa este medio de teletrabajo.	Al no tener presente este tipo de activo se excluye el control

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
7. seguridad en los recursos	7.1	Previo al empleo			
	7.1.1	Verificación de antecedentes	Si		Sugiere realizar la constatación de los antecedentes del personal lo cual podrá filtrar aquellas personas que represente un riesgo para la entidad
	7.1.2	Términos y condiciones de empleo	Si		Se sugiere diseñar y establecer las condiciones de empleo, las que tienes que ser comunicados a previo contrato de empleo en pro de la seguridad de la información
	7.2	Durante el empleo			

	7.2.1	Responsabilidad de la alta gerencia	Si		Se sugiere hacerle conocer a la alta gerencia de su rol y su responsabilidad en el sistema de gestión de seguridad de la información para que su participación sea frecuente.
Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
7. seguridad en los recursos	7.2.2	Conciencia, educación y capacitación	Si		Se sugiere que debe haber un plan en donde se toque tema de conciencia, educación y capacitación que nos servirá para la seguridad de la información
	7.2.3	Sanciones en la Seguridad de la información	Si		Poner sanciones a las personas que infrinjan la seguridad de la información

	7.3	Termino y cambio de empleo			
	7.3.1	Termino de responsabilidades	Si		Los trabajadores deben acatar las condiciones de empleo actuales esto para beneficio de la entidad en temas de seguridad de la información

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
8. gestión de activos	8.1	Responsabilidad de activos			
	8.1.1	Inventario de activos	Si		Se sugiere que la información que le brindan a la entidad de DRTCA sea clasificada para posterior evaluación según su clasificación
	8.1.2	Propiedad de los activos	Si		Se sugiere que los activos tengan dueños claros responsabilidades y así la protección de los activos se más segura
	8.1.3	Uso aceptable de activos	Si		Se sugiere que exista un procedimiento para el uso aceptable de los activos que es beneficioso en la seguridad de la información y hacerla conocer al responsable.

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
8. gestión de activos	8.2	Clasificación de la información			
	8.2.1	Clasificación de la información	Si		Se sugiere clasificar a los activos de información según su confidencialidad, integridad y disponibilidad
	8.2.2	Etiquetado de la información	Si		Después de clasificar se debe etiquetar en sentido que todos lo reconozcan como información sensible
	8.2.3	Manejo de activos	Si		Se sugiere tener un correcto uso de la información para lo cual ayuda el etiquetado y clasificado
	8.3	Manejo de medios	Si		
	8.3.1	Gestión de medios removibles	Si		Se sugiere establecer procedimientos que sea acorde a las necesidades para

					medios extraíbles como son USB
	8.3.2	Eliminación de medios	Si		Se sugiere el correcto manejo de eliminación
Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
8. gestión de activos	8.3.3	Transporte de medios físicos	Si		Se sugiere establecer reglas que aseguren la información física de forma que el activo no sea manipulable
9. control de acceso	9.1	Requerimiento de negocio para el control de acceso			
	9.1.1	Política de control de acceso	Si		Se sugiere que las políticas de control de acceso deben estar difundida por todos y cumpliendo
	9.1.2	Políticas en el uso de servicio de red	Si		Se sugiere tener políticas en cuanto al uso del servicio de la red
	9.2				

	9.2.1	Registro y baja del usuario	Si		Se sugiere tener actualizado y controlado para poder estar monitoreando los usuarios
	9.2.2	Gestión de privilegios	Si		Se sugiere establece una adecuada gestión de privilegios en activos
Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
9. control de acceso	9.2.3	Gestión de información de autenticación secreta de usuario	No	Los trabajadores cuentan con autentificación como lo es un password en el área de brevetes	Al existir el control se excluye
	9.2.4	Revisión de derechos de acceso de usuario	Si		Se sugiere que la asignación de la información de password debe ser gestionada
	9.2.5	Eliminación o ajuste de derechos de acceso	Si		Se sugiere que los propietarios deberían revisar los accesos

	9.3	Responsabilidades del usuario			
	9.3.1	Uso de información de autenticación secreta	Si		Se sugiere a los trabajadores tener en consideración las buenas prácticas en seguridad de la información
	9.4	Control de acceso de sistemas y aplicaciones			
	9.4.1	Restricción de acceso a la información	No	Los trabajadores cuentas con acceso de usuario y contraseña por tanto se restringe	Al existir el control se excluye
Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
9. control de accesos	9.4.2	Procedimiento de inicio de sesión segura	Si		Se sugiere que cuando se inicie de forma de sesión segura se debería tener controlado manejar algunas aplicaciones todo aquello para proteger la información

	9.4.3	Sistema de gestión de contraseña	Si		Se sugiere que las contraseñas sean gestionadas de manera que cumplan con los requisitos mínimos
	9.4.4	Uso de programas y utilidades privilegiadas	Si		Se sugiere que el uso de programas sea muy controlado que podría cuásar daño a los activos de información
	9.4.5	Control de acceso al código fuente del programa	Si		Se sugiere restringir el acceso al código fuente de las aplicaciones

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
10. cifrado	10.1	Controles criptográficos			
	10.1.1	Restricción de acceso a la información	Si		Se sugiere tener procedimientos cifrados que restringa a la información sensible
	10.1.2	Procedimiento de inicio de sesión segura	Si		Se sugiere contar con gestión de claves y enunciar los responsables
11. seguridad física y del entorno	11.1	Áreas seguras			
	11.1.1	Perímetro de seguridad física	No	Los documentos que ingresan a un área se hacen responsable el jefe de esa área	Al existir el control se excluye
	11.1.2	Controles físicos de entrada	No	Se cuenta con personal en las puertas de ingreso para las oficinas	Al existir el control se excluye
	11.1.3	Seguridad de oficinas, despachos y recursos	Si		Se sugiere tener un sistema de seguridad físicas en las diferentes áreas

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
11. Seguridad física y del entorno	11.1.4	Protección contra amenazas externas y del ambiente	Si		Se sugiere tener un plan ante desastres físicas naturales que puedan alterar los activos
	11.1.5	Trabajo en áreas seguras	Si		Se sugiere diseñar áreas de trabajo seguras en pro de la seguridad de la información
	11.1.6	Áreas de acceso público, entrega y carga	Si		Se sugiere que el área al acceso al público se espacioso y controlado
	11.2	Intercambio de información con partes externas			
	11.2.1	Instalación y protección de equipos	Si		Se sugiere que los equipos deben protegerse contra amenazas
	11.2.2	Servicio de soporte	Si		Se sugiere contar con suministro de energía eléctrica alterna

	11.2.3	Seguridad en el cableado	Si		Se sugiere que los cables de datos estén en conste mantenimiento y cuidado

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
11. Seguridad física y del entorno	11.2.4	Mantenimiento de equipo	Si		Se sugiere que los equipos que almacenas información critico tengan un programa de mantenimiento
	11.2.5	Retiro de activos	Si		Se sugiere que la entidad debe estableces políticas de retiro de activos
	11.2.6	Seguridad de equipo y activos fuera de instalación	Si		Se sugiere que la entidad haya identificado a las personas que tiene alguna relación externa.

	11.2.7	Eliminación segura o reusó del dispositivo de almacenamiento	Si		Se sugiere que los equipos informáticos que se den de baja deben pasar por un proceso de limpieza para continuar en operación
	11.2.8	Equipo informático de usuario desatendido	Si		Se sugiere que los trabajadores deben mantener la seguridad de sus equipos aun estos no funcionen
Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
11. seguridad física y del entorno	11.2.9	Política del puesto de trabajo despejado y bloqueado de pantalla	Si		Se sugiere que los trabajadores no tengan activos sensibles en sus escritorios esto en pro de la seguridad de la información
12. seguridad operativa	12.1	Responsabilidades y procedimiento de operación			

	12.1.1	Documentación de procedimiento de operación	Si	Se cuenta con documentos de procedimientos	Al existir el control se excluye
	12.1.2	Gestión de cambios	Si		Se sugiere que se realice la gestión de cambios en los activos de información periódicamente
	12.1.3	Gestión de capacidades	Si		Se sugiere monitorear el uso de recurso para garantizar el rendimiento adecuado
	12.1.4	Separación de entornos de desarrollo, prueba y producción	Si	Las áreas están separadas y bien definidas	Al existir el control se excluye
	12.2	Protección contra código malicioso			

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
12. seguridad de la operativa	12.2.1	Controles contra el código malicioso	Si		Se sugiere proponer un plan para la detección de malware código malicioso en

					coordinación con cada área
	12.3	Copias de seguridad			
	12.3.1	Copias de seguridad de la información	Si		Se sugiere tener un programa de copias de seguridad de la información y programas
	12.4	Registro de actividad y supervisión			
	12.4.1	Registro y gestión de eventos de actividades	Si		Se sugiere tener un registro de eventos actividades de cualquier tipo de fallas
	12.4.2	Protección de los registros de información	Si		Se debería proteger la información contra cualquier acceso no autorizado

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
12. seguridad operativa	12.4.3	Registro del administrador y operador del sistema	Si		Se sugiere registrar las actividades del que se dan en cada momento del examen teórico
	12.4.4	Sincronización de relojes	Si		Se sugiere sincronizar los relojes de todos los sistemas de procesamiento de dato con una fuente única
	12.5	Control del software en explotación			
	12.5.1	Instalación del software en sistema en producción	Si		Se sugiere diseñar procedimientos para controlar la instalación de software de los sistemas operativos
	12.6	Gestión de la vulnerabilidad técnica			
	12.6.1	Gestión de las vulnerabilidades técnicas	Si		Se sugiere tener un plan para la evaluación periódica sobre las vulnerabilidades que afectan a los activos

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
12. seguridad operativa	12.6.2	Restricciones en la instalación de software	Si	está prohibido instalar programas nuevos sin previa evaluación de área encargada	Al existir el control se excluye
	12.7	Consideraciones de las auditorias de los sistemas de información			
	12.7.1	Controles de auditoria de los sistemas de información	Si		Se sugiere que se debería planificar las auditorias en todas las computadoras del área de brevetes
13. seguridad en las telecomunicaciones	13.1	Gestión de la seguridad en las redes			
	13.1.1	Controles de red	Si		Se sugiere que se debería controlar la red para proteger la información
	13.1.2	Mecanismo de seguridad asociados a servicios en red	Si		Se sugiere incluir en el contrato de los servicios los mecanismos de seguridad a la red

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
13. seguridad en las telecomunicaciones	13.1.3	Segregación de redes	Si	Las redes están desagregadas de acuerdo al área	Al existir el control se excluye
	13.2	Intercambio de información con partes externas			
	13.2.1	Políticas y procedimientos de intercambio de información	Si		Se sugiere que deberían haber acuerdo con las entidades externas en la transferencia de información segura
	13.2.2	Acuerdo de intercambio	Si		Se sugiere que los acuerdo con las entidades externas deben ser seguras previo acuerdo
	13.2.3	Mensajería electrónica	No		No se considera este control ya que no se cuenta con este servicio
	13.2.4	Acuerdo de confidencialidad y secreto	Si		Se sugiere identificar, revisar los activos de forma periódica

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
14. adquisición desarrollo y mantenimiento de los sistemas de información	14.1	Requisitos de seguridad de los sistemas de información			
	14.1.1	Análisis y especificaciones de los requisitos de seguridad	Si		Se sugiere que los requisitos relacionados con la seguridad de la información deben plasmar también para los nuevos equipos
	14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes publicas	Si		Se sugiere que proteger la información que pasa por servicios externos
	14.1.3	Protección de las transacciones por redes telemáticas	No	No hay	No se considera el control porque no se cuenta con ese servicio
	14.2	Seguridad en los procesos de desarrollo y soporte			
	14.2.1	Política de desarrollo seguro de software	Si		Se sugiere establecer reglas para el desarrollo de software

					dentro del área de brevete
	14.2.2	Procedimiento de control de cambios en los sistemas	Si		Se sugiere tener un plan de ciclo de vida del software

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
14. adquisición desarrollo y mantenimiento de los sistemas de información	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambio en el sistema operativo	Si		Se sugiere que las aplicaciones críticas para el servicio se deberán revisar y probar para garantizar que no se ha generado impactos adversos
	14.2.4	Restricciones a los cambios en los paquetes de software	Si		Se sugiere limitar los cambios de configuración de los paquetes de software

	14.2.5	Uso de principios de ingeniería en protección de sistemas	Si		Se sugiere establecer principios de seguridad de ingeniería para la implementación
	14.2.6	Seguridad en entornos de desarrollo	Si		Se sugiere proteger los entornos del desarrollo de la seguridad de la información
	14.2.7	Externalización del desarrollo de software	Si		Se sugiere monitorear los desarrollos de software externalizados
	14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	Si		Se sugiere hacer pruebas en la etapa del desarrollo del software

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
14. adquisición, desarrollo y mantenimiento de los sistemas de información	14.2.9	Pruebas de aceptación	Si		Se sugiere hacer pruebas de aceptación del software
	14.3	Datos de prueba			
	14.3.1	Protección	Si		Se sugiere que los datos de pruebas se deberían seleccionar cuidadosamente y se deberían controlar y proteger
15. relaciones con suministradores	15.1.1	Seguridad de la información en las relaciones con suministros			
	15.1.1	Política de seguridad de la información para suministros	Si		Se sugiere establecer acuerdos para poder proteger los activos para los suministros
	15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	Si		Se sugiere tener la documentación sobre la seguridad a los suministrados

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
15. relaciones con suministradores	15.1.3	Cadena de suministro e n tecnologías de la información y comunicación	Si		Se sugiere que exista acuerdos que aborden los riesgos de información asociados al servicio
	15.2	Gestión de la prestación del servicio por suministradores			
	15.2.1	Supervisión y revisión de los servicios prestados por terceros	Si		Se sugiere que la entidad debe monitorear a la prestadora de servicio
	15.2.2	Gestión de cambios en los servicios prestados por terceros	Si		Se sugiere tener controlado los cambios en la prestación de servicios
16. gestión de incidentes en la seguridad de la información	16.1	Gestión de incidentes de la seguridad de la información y mejoras			
	16.1.1	Responsabilidades y procedimientos	Si		Se sugiere planificar las respuestas antes impacto negativos en los activos de información

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
16. Gestión de incidentes en la seguridad de la información	16.1.2	Notificaciones de los eventos de seguridad de la información	Si		Se sugiere informar ante un evento malicioso
	16.1.3	Notificaciones de puntos débiles de seguridad de la información	Si		Se sugiere que debería anotar los puntos débiles de la información
	16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	Si		Se sugiere valorizar los eventos negativos para posterior análisis y tomas de decisión
	16.1.5	Respuestas a los incidentes de seguridad	Si		Se sugiere tener un plan de respuestas de incidentes para la seguridad de información
	16.1.6	Aprendizaje de los incidentes de seguridad de la información	Si		Se sugiere aprender de la experiencia para lo cual debe haber una mejora continua
	16.1.7	Recopilación de evidencias	Si		Se sugiere tener evidencias de eventos maliciosos

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
17. aspectos de seguridad de la información en la gestión de la continuidad del negocio	17.1	Continuidad de la seguridad de la información	Si		
	17.1.1	Planificación de la continuidad de la seguridad de la información	Si		Se sugiere planificar las acciones ante desastres
	17.1.2	Implementación de la continuidad de la seguridad de la información	Si		Se sugiere implementar un plan de seguridad de la información
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Si		Se sugiere monitorear los controles de seguridad de información
	17.2	Redundancias			
	17.2.1	Disponibilidad de instalaciones para el procedimiento de la información	Si		Sugiere para los procedimientos de seguridad de la informa
Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION

18. cumplimiento	18.1	Cumplimiento de los requisitos legales y contractuales	Si		
	18.1.1	Identificación de la legislación aplicables	Si		Se sugiere identificar la legislación que afecten al área
	18.1.2	Derechos de propiedad intelectual	Si		Se sugiere tener procedimiento para identificar los derechos intelectuales
	18.1.3	Protección de los registros de la organización	Si		Se sugiere proteger los registros de información
	18.1.4	Protección de datos y privacidad de la información personal	Si		Se sugiere proteger la información personal
	18.1.5	Regulación de los controles criptográficos	Si		Se sugiere usar controles criptográficos para asegurar la información

Anexo A de la NTP-ISO/IEC 27001: 2014					
CLAUSULA	SECCION	OBJETIVO DE CONTROL	APLICABILIDAD	CONTROL ACTUAL	JUSTIFICACION
18. cumplimiento	18.2	Revisiones de la seguridad de la información			
	18.2.1	Revisión independiente de la seguridad de la información	Si		Se recomienda monitorear el plan de seguridad de la información
	18.2.2	Cumplimiento de las políticas y normas de seguridad	Si		Se sugiere que los responsables de cada área deben velar por el cumplimiento de la seguridad de la información
	18.2.3	Comprobación del cumplimiento	Si		Se sugiere monitorear los controles para su buen funcionamiento

ANEXO MATRIZ DE CONSISTENCIA

PROBLEMA		HIPÓTESIS		OBJETIVO	
General	**Específicos**	**General**	**Nula**	**General**	**Específicos**
¿Cómo la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 mitigara los siniestros de los activos de información en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash?	P1: ¿De qué manera la declaración de aplicabilidad mitigara el daño de los siniestros de la información mediante el contexto de la organización de la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash? P2: ¿De qué manera la declaración de aplicabilidad mitigara el daño de los siniestros de la información mediante la planificación de la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash?	Con la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 se mitigará los siniestros de los activos de información en la subdirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash.	Con la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 no se mitigará los siniestros de los activos de información en la subdirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash.	Conocer cómo la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 mitigara los siniestros de los activos de información en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash.	O1. Establecer de qué manera la declaración de aplicabilidad mitigara el daño de los siniestros de la información mediante el contexto de la organización de la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash. O2. Establecer de qué manera la declaración de aplicabilidad mitigara el daño de los siniestros de la información mediante la planificación de la NTP-ISO/IEC 27001:2014 en la sub dirección de licencias de conducir de la DRTCA

ANEXO: REPOSITORIO INSTITUSIONAL DE LA UNASAM

1. Datos del Autor:

Apellidos y Nombres: Jose Antonio Quispe Barreto

Código de alumno: 061.125.377 Teléfono: 916140392

Correo electrónico: jose_ant.15@hotmail.com DNI: 44943018

2. Modalidad de trabajo de investigación:

( ) Trabajo de Investigación ( ) Trabajo académico

( ) Trabajo de suficiencia personal (X) Tesis

3. Título profesional o grado académico

( ) Bachiller (X) Titulo ( ) Segunda especialidad

( ) Licenciado ( ) Magister ( ) Doctor

4. Título del trabajo de investigación

"DECLARACIÓN DE APLICABILIDAD MEDIANTE LA NTP-ISO/IEC27001:2014 PARA MITIGAR LOS SINIESTROS DE LA INFORMACIÓN EN LA SUB DIRECCIÓN DE LICENCIAS DE CONDUCIR DE LA DIRECCIÓN REGIONAL DE TRANSPORTE Y COMUNICACIÓN DE ÁNCASH, 2018"

5. Facultad de: Ciencias

6. Escuela, Carrera o programa: Escuela Profesional de Ingeniería de Sistema e Informática.

7. Asesor:

Apellidos y Nombres: Ing. Flores Chacón Erick Giovanny Teléfono: 956963007

Correo electrónico: gflores_ing@hotmail.com DNI: 07964931

A través de este medio autorizo a la Universidad Nacional Santiago Antúnez de Mayolo, publicar el trabajo de investigación en formato digital en el Repositorio Institucional Digital, Repositorio Nacional Digital de Acceso Libre (ALICIA) y el Registro Nacional de Trabajos de Investigación (RENATI).

Asimismo, por la presente dejo constancia que los documentos entregados a la UNASAM, versión impresión y digital, son las versiones finales del trabajo sustentado y aprobado por el jurado y son de autoría del suscrito en estricto respeto a la legislación en materia de propiedad intelectual

Firma: .....

DNI: 44943018

FECHA: 07 de Enero de 2019.