Universidad Continental

FACULTAD DE INGENIERÍA

Escuela Académico Profesional de
Ingeniería de Sistemas e Informática

Tesis

Diseño de un modelo de gestión de seguridad de la información con un enfoque en el factor humano para el ICPNA Región Centro en el año 2017

Iván Antonio Pizarro Sánchez

Huancayo, 2018

Para optar el Título Profesional
de Ingeniero en Sistemas e Informática

AGRADECIMIENTOS

El presente trabajo requiere un agradecimiento especial a la Universidad Continental por su apoyo y soporte en la elaboración del trabajo de investigación, así como por las facilidades brindadas para la elaboración de la investigación. Asimismo, es necesario agradecer al ICPNA Región Centro por la información brindada para la elaboración del estudio, sin la cual el trabajo hubiera sido imposible.

De forma particular quisiera agradecer a mi asesor Dr. Job Daniel Gamarra Moreno por su incondicional apoyo en la elaboración y revisión exhaustiva de este trabajo. Del mismo modo, quisiera agradecer al Ing. Martín Valdivia Benites por su asesoría y consejos sobre la dirección del estudio de investigación que me permitieron tener un rumbo adecuado de investigación. También, quisiera agradecer al Dr. Jacinto Arroyo Aliaga por su apoyo en la parte organizativa y metodológica. Por último, quisiera agradecer al Ing. Miguel Tupac Yupanqui Alanya por sus consejos y apoyo para poder realizar este trabajo. Las palabras y acciones de cada uno de ellos me animaron constantemente y fueron parte del empuje necesario en la culminación de esta labor.

DEDICATORIA

Quisiera dedicar este trabajo, en primer lugar, a Dios quien es aquel que me dirige a cada instante para dar lo mejor de mí en cada proyecto que emprendo y cuya enseñanza me hace ser un mejor hombre cada día.

También dedico este trabajo a mi esposa, mis padres, mi familia, mis profesores y todos aquellos que hicieron posible este esfuerzo con su apoyo y constante fe en lo que podía llegar a lograr.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

En el ámbito de la seguridad de la información, se ha detectado en los últimos años que, a pesar de tener medidas tecnológicas para contrarrestar los ataques contra la integridad, disponibilidad y confiabilidad de la información en las empresas, el factor humano sigue siendo uno de los problemas más difíciles de combatir. Este estudio tecnológico tuvo como propósito diseñar un modelo de seguridad de la información que tenga un enfoque en el factor humano de la seguridad de la información para el ICPNA (Instituto Cultura Peruano Norteamericano) Región Centro y que permita también fortalecer dicho factor. El estudio tiene un diseño no experimental de tipo transversal puesto que para la elaboración del modelo se realizó un estudio previo a la institución en cuestión y luego se realizó una investigación sobre las diferentes teorías de comportamiento que pueden relacionarse con la seguridad de la información, así como a los estándares de seguridad de la información actuales y por medio del método analítico-sintético se logró consolidar un modelo de seguridad que contempla el factor humano en todo su ciclo de desarrollo a partir de literatura relacionada al tema e información recopilada en la empresa. El resultado del estudio es un modelo de seguridad de la información que permite el fortalecimiento del factor humano y que se orienta a gestionar y proteger la información dentro del ICPNA Región Centro según los estándares y normativa vigente. Entre las conclusiones de la tesis se menciona que existe una necesidad latente de gestionar la seguridad de la información en la institución; así también que el modelo de Seguridad de la Información considera información relevante para el ICPNA Región Centro, por lo cual ayudará a fortalecer la seguridad de la información del factor humano, dar tratamiento a los riesgos de seguridad de la información y gestionar la seguridad de la información dentro de la empresa; sin embargo, la implantación de dicho modelo no será parte del estudio actual.

ABSTRACT

In the information security world, it has been detected that in the last years, and despite having technological measures to fight the attacks against businesses' information integrity, availability and confidentiality, the human factor is still being one of the most difficult to combat problems. The purpose of the study was to develop an information security model that has a focus on the human factor of information security for the ICPNA Región Centro. The study has a non-experimental design and its type is transversal since for the elaboration of the model a previous study to the institution was made and then there was an investigation on the different theories of behavior that can be related to the security of the information, as well as the current information security standards that helped shape the model. Through the analytic-synthetic method, a security model which considers the human factor throughout its development cycle was consolidated based on literature related to the topic and information gathered in the company. The project result is a model of information security that allows the strengthening of the human factor which is also oriented to manage and protect the information within ICPNA Región Centro according to current standards and regulations. Among the project's conclusions, it is concluded that there is a latent need to manage information security in the institution; also, the information security model considers relevant information for the ICPNA Región Centro; therefore, it will strengthen the human factor's information security; it will give treatment to the information security risks, and it will manage information security within the company; however, the implementation of this model was not part of the actual study.

INTRODUCCIÓN

La seguridad de la información es en la actualidad uno de los temas de mayor preocupación entre los profesionales de sistemas de información a nivel mundial. A partir del incremento de las tecnologías de la información a nivel mundial y de la interconexión de dispositivos relacionados a través de Internet, se han venido desarrollando sistemas de información que permiten que las empresas puedan lograr una presencia sin precedentes, no sólo a nivel local, sino a nivel internacional; esto ha traído como resultado un incremento en la dependencia de las compañías que hoy en día deciden mantener su información en medios computacionales como servidores locales y hasta en la nube; además, el acceso a información desde lugares distantes por medio del uso de las redes de telecomunicaciones hace posible la existencia de nuevas oportunidades para las empresas a nivel mundial tal es el caso del ICPNA Región centro.

Sin embargo, los mismos beneficios que brinda el uso de tecnologías de la información y el libre flujo de información a través de redes de computadora a nivel mundial por medio del uso de la Internet, también facilita que los denominados criminales informáticos pretendan aprovechar dichas tecnologías para cometer crímenes de índole económico, personal y de reputación en contra de personas y empresas. Por consiguiente, en los últimos años ha existido un incremento en la producción de tecnologías que permitan asegurar la seguridad, integridad y confidencialidad de la información de las empresas y asegurar que el uso de la información es el correcto y adecuado. Sin embargo, a pesar de los esfuerzos de implementar tecnología, se ha descubierto que son los propios usuarios de los sistemas los que facilitan el trabajo de los criminales informáticos por medio de actitudes inseguras que la tecnología no puede controlar.

Es por este motivo que en la actualidad existe un énfasis en la formación y la modificación del comportamiento de los trabajadores dentro de las empresas para fortalecer el eslabón más débil de la seguridad de la información, los usuarios. Por lo tanto, el estudio plantea un modelo de seguridad de la información basado en estándares internacionales y teorías sociales y psicológicas que ayuden a fortalecer el factor humano de la seguridad de la información al proponer etapas de implementación de un modelo que permite un fortalecimiento continuo del factor humano dentro del ICPNA Región Centro que requiere implementar una gestión de la seguridad de la información.

Para la realización del modelo se utilizó una perspectiva sistémica para poder analizar de forma holística el nivel de la seguridad de la información en la empresa mencionada; además, se utilizó una metodología analítica y sintética que permitió generar un modelo de seguridad de la información a partir de la información obtenida. Del mismo modo, se tuvo en consideración el modelo de ciclo de calidad de Deming como una propuesta de mejora continua para el modelo. La investigación fue de tipo tecnológico porque se aplicaron criterios de seguridad de la información del ISO/IEC 27002:2013, MAGERIT v.3, Norma Técnica Peruana NTP-ISO/IEC 27001 y ley 29733, para resolver el problema de comportamiento inseguro en los usuarios de los sistemas; también tiene un nivel descriptivo porque se describió como se debe implementar el modelo de seguridad y aplicativo debido a que se utilizaron teorías relacionadas al comportamiento humano para la gestión de seguridad de la información.

En el primer capítulo se realiza el planteamiento del problema de investigación considerando información sobre seguridad de la información a nivel global, nacional, y dentro del ICPNA Región Centro; a partir de lo cual se formula el problema general y los problemas específicos del estudio que determina la necesidad de fortalecer el factor humano en la seguridad de la información; además, se establecen los objetivos del estudio. Posteriormente, se establece la relevancia del estudio a través de la justificación académica, científica y tecnológica para el estudio y se procede a delimitar el problema. El capítulo finaliza con los entregables del estudio.

En el segundo capítulo se brindan los antecedentes de investigación del estudio y se consideran artículos científicos, tesis de grado y de maestría, artículos de revistas especializadas y la opinión de un experto en la materia. Luego se exponen las bases teóricas que servirán como fundamento para la elaboración del modelo de seguridad de la información donde se consideran teorías psicológicas y sociales como la teoría de necesidades básicas, teoría de comportamiento planificado y teoría de control social, así como el ISO/IEC 27002:2013, MAGERIT v.3, Norma Técnica Peruana NTP-ISO/IEC 27001 y ley 29733 para la elaboración del modelo de seguridad. El capítulo concluye con la definición de términos básicos.

En el tercer capítulo se describe la metodología de estudio considerando los métodos generales y específicos, el alcance de la investigación teniendo en cuenta el tipo y nivel del mismo y su consecuente diseño. Adicionalmente se describen el caso de estudio y las técnicas e instrumentos para la recolección de la información como base para la elaboración del modelo de seguridad.

En el cuarto capítulo se muestra información recopilada y permitida de publicar por la empresa, previa al modelo, obtenida de los checklists, encuestas, entrevistas desarrollados a 37 trabajadores entre personal administrativo y docente dentro del ICPNA Región centro. En la segunda parte del capítulo se presenta el modelo de seguridad de la información y las fases necesarias dentro del ciclo de desarrollo del modelo a partir de los estándares usados.

CAPÍTULO I

PLANTEAMIENTO DEL ESTUDIO

1.1 Caracterización y formulación del problema

1.1.1 Caracterización del problema

Un aumento exponencial del uso de tecnologías de la información dentro de las empresas como un factor relevante para su desarrollo se ha producido en los últimos años. Es este incremento parte del plan de desarrollo de instituciones a nivel mundial como la ONU (Organización de las Naciones Unidas) cuya preocupación por formar sociedades de la información y fomentar el intercambio a nivel global. Asimismo, se observa que la llamada revolución digital en el incremento de uso de las tecnologías de información y las telecomunicaciones ha permitido un flujo abierto y libre de información en todo el mundo (Tellez, 2008). Por lo tanto, las empresas que anhelan permanecer competitivas se ven en la obligación de utilizar las diversas tecnologías de la información y comunicaciones para el manejo de su información.

El Perú no es exento de esta realidad; estudios del INEI revelan que un 95.1% de las empresas en el país tienen computadoras, y un 92.7% de empresas cuentan con acceso a Internet. Así también se evidencia que un 76.6% empresas cuenta con redes de área local y cuentan con dispositivos que les ayudan a compartir información y recursos (INEI, 2009). Esto demuestra una creciente demanda de las empresas en nuestro país por mantenerse competitivas debido a los múltiples beneficios que le brindan las TICS a su evolución.

Sin embargo, es de conocimiento público que dichas tecnologías de la información brindan el acceso, tratamiento y producción y divulgación de la información contenida en ellos (Beloch, 2011), y pueden ser una ocasión de acceso a personas autorizadas o no autorizadas para que de forma malintencionada o por descuido afecten la integridad, confidencialidad y disponibilidad de la información de las empresas. Es por este motivo que la seguridad de la información se ha convertido en un área de constante desarrollo y desafío para los profesionales de las TICS.

Según estudios de la OEA (Organización de Estados Americanos) recopilados por Symantec, Sudamérica se registra en estos últimos años los más altos índices de crecimiento en conectividad en todo el mundo. Esto significa que existen más dispositivos, servicios, usuarios, redes de comunicación, y también más sistemas, lo cual significa también muchos más beneficios y oportunidades para las personas. No obstante, esto también significa tener más vulnerabilidades y amenazas, lo que conlleva a tener mayores costos y mayor número de víctimas (Symantec, 2014).

En el Perú, según un informe emitido por el Ministerio de la Producción, se evidenció que existe un 99,5% de micro, pequeñas y medianas empresas (MIPYMES) y estas empresas han reportado un crecimiento anual de 7,6% entre los años 2009 y 2013 (Dirección General de Estudios Económicos, Evaluación y Competitividad Territorial del Viceministerio de Mype e Industria, 2014). Asimismo, el porcentaje de uso de la las TICS en dichas empresas peruanas aumentó en los últimos años, así como lo confirma un estudio realizado por el Consejo Nacional de la Competitividad donde menciona que un 75% de las MYPE utilizan TIC y cuentan con servicios de Internet (Aguilar, 2014).

Del mismo modo, según un estudio realizado por INEI sobre el uso de internet, intranet y extranet, el uso de internet en pequeñas empresas tal es el caso del ICPNA Región Centro, se obtuvo un incremento de 82,44% en el 2011 a 87,1% en el 2015 (INEI, 2015) lo cual se muestra en la figura 1.

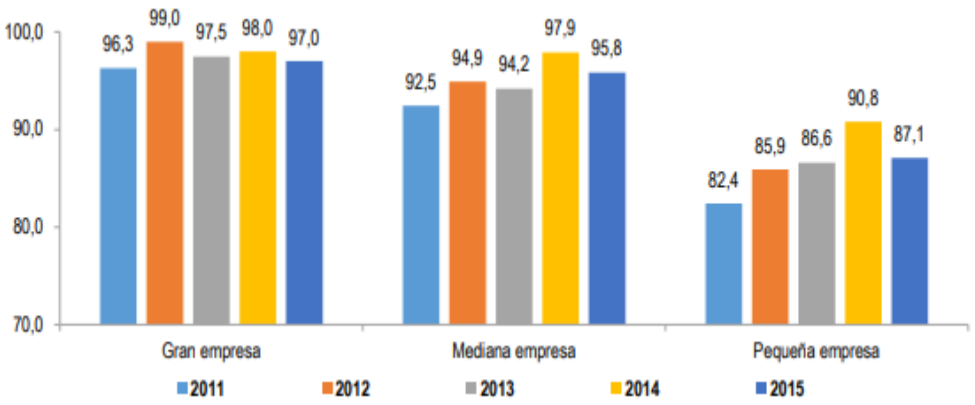

Figura 1. Empresas que utilizaron internet, según segmento empresarial (2011-15) (porcentaje)

Fuente: Instituto Nacional de estadística e informática. (INEI, 2015)

De la misma manera, las empresas como el ICPNA han aumentado su uso de internet, también han aumentado su uso de intranet y extranet tal como lo muestran las figuras 2 y 3 respectivamente. De las cuales se evidencia que hubo un incremento de 3% en el uso de intranet a nivel nacional; en el caso del ICPNA Región centro esto se hace también evidente por el uso de su intranet y extranet para gestión docente y administrativa.

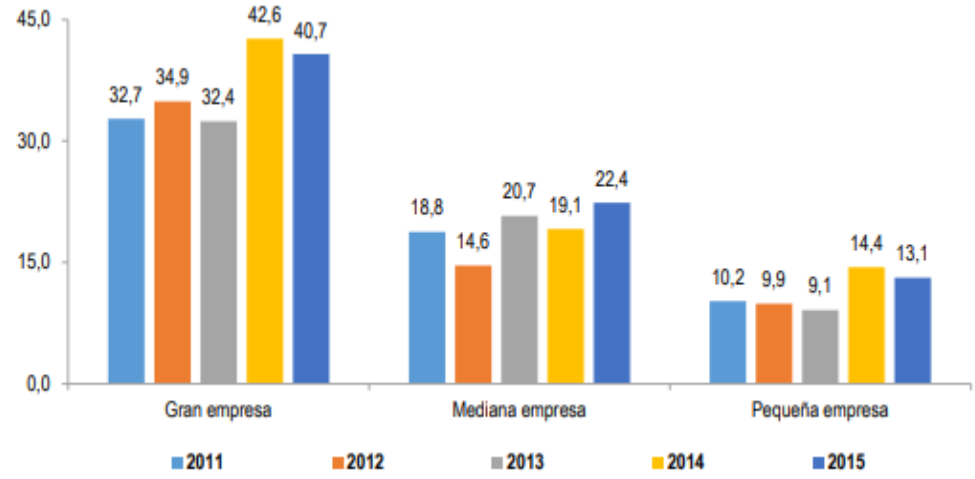

Figura 2. Empresas que utilizaron intranet, según segmento empresarial (2011-15) (porcentaje)

Fuente: Instituto Nacional de estadística e informática. (INEI, 2015)

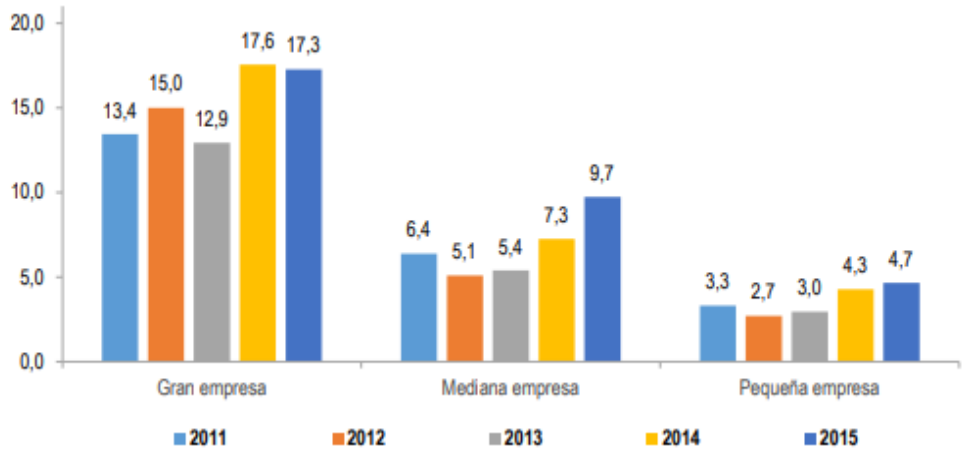

Figura 3. Empresas que utilizaron extranet, según segmento empresarial (2011-15) (porcentaje)

Fuente: Instituto Nacional de estadística e informática. (INEI, 2015)

Por otro lado, en el ámbito de gestión de la seguridad de la información es conocido que el factor humano es el punto más vulnerable y más difícil de fortalecer para evitar ataques informáticos. El 2012 se detectó que dos terceras partes (64%) de las fugas de información fueron ocasionadas por el error humano, por un inadecuado manejo de información confidencial, por infracción a las normativas y por falta de controles a los usuarios (SealPath, 2015). Según SealPath, las fugas de información más comunes relacionadas al factor humano son: el error y despiste humano, uso malintencionado de la información e ingeniería social (Symantec, 2014).

Esta información se reafirma con la tendencia en vulnerabilidades en los sistemas informáticos a nivel global realizada por Symantec para Latinoamérica; el aumento de vulnerabilidades encontrados en los sistemas de información es realmente preocupante para las empresas que ven su información en riesgo debido a estos cambios. La figura 4 ilustra esta tendencia donde se muestra el número de vulnerabilidades encontradas cada año en los sistemas informáticos donde un número significativo de ellas se relaciona con el factor humano.

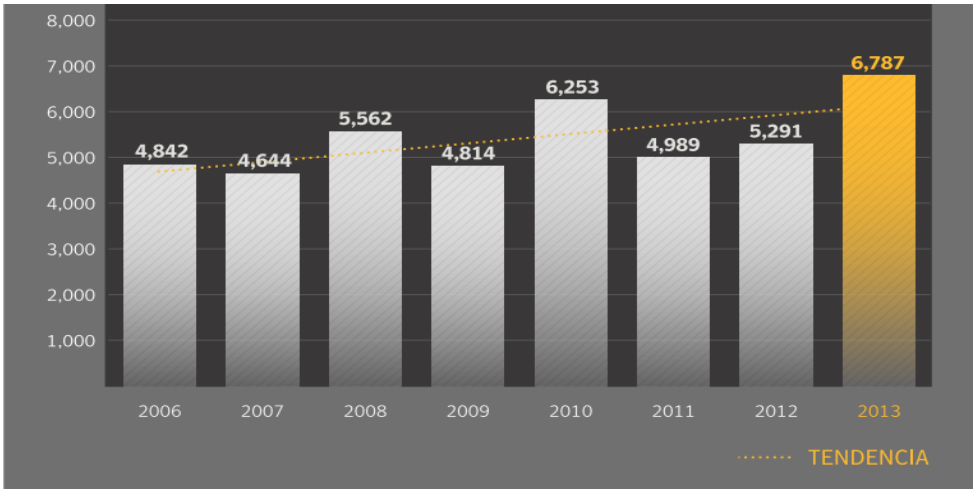

Figura 4. Tendencia de vulnerabilidades en los sistemas

Fuente: (Global), 2006 – 2013. (Symantec, 2014)

En otro estudio realizado por EY Perú, se evidenció que de las empresas en el Perú, un 90% de los ataques proviene de los propios empleados y un 68% de hackers como se observa en la figura 5. Además, se concluyó que los dos principales causantes de vulnerabilidades son los colaboradores imprudentes o poco concientizados y los controles obsoletos de la seguridad de la información como se ve en la figura 6 (EY-Perú, 2015).

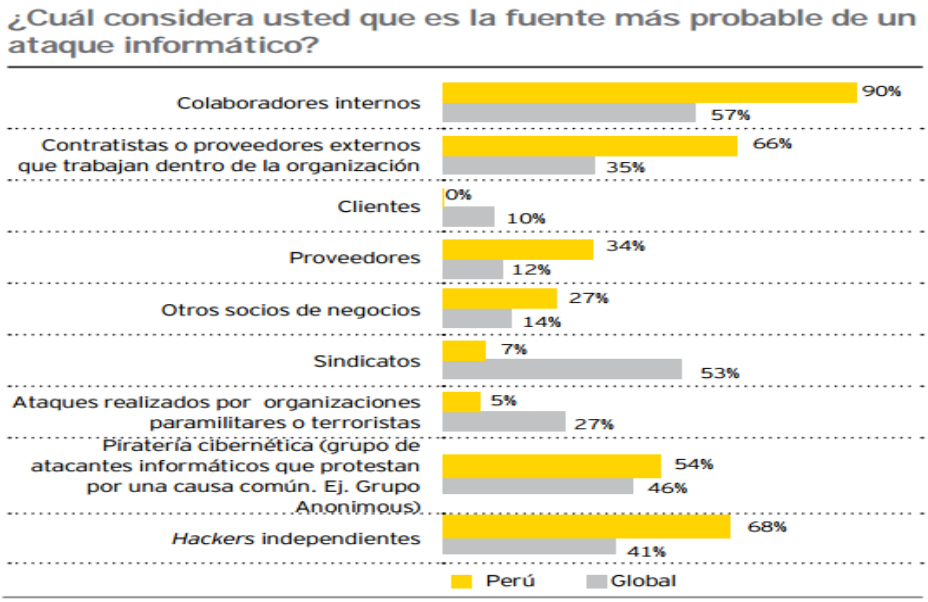

Figura 5. Fuente más probable de ataque informático.

Fuente: (EY-Perú, 2015)

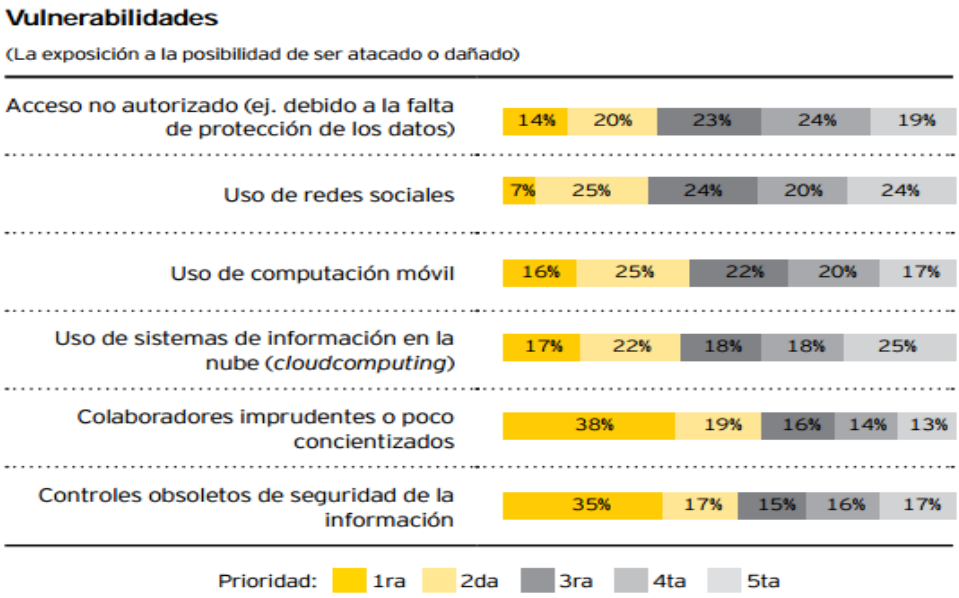

Figura 6. Proveniencia de vulnerabilidades en las empresas.

Fuente: (EY-Perú, 2015)

Asimismo, se ha descubierto que un 68 % de las organizaciones en el Perú no incluye seguridad de la información en la evaluación a sus empleados; mientras que un 71% ve un incremento de riesgo de amenazas externas. Sin embargo, lo más preocupante es el porcentaje tan bajo de empresas dispuestas a invertir en su propia seguridad de la información (EY-Perú, 2015). Esto nos muestra la realidad de nuestras empresas con respecto a su propio nivel de seguridad de la información.

Si bien es cierto, cada compañía que produce tecnología relacionada con la información tiene en consideración los estándares, guías, marcos de referencia y mejores prácticas que han dejado años de experiencia en combatir los ataques informáticos a nivel mundial; No obstante, son las propias empresas las que no invierten en su seguridad, y a su vez, son los propios usuarios de los sistemas en la empresas aquellos que facilitan la labor de los criminales informáticos a través de sus falta de conocimiento de seguridad de la información. Ante esta disyuntiva, es necesario e indispensable asegurar la información de forma individualizada.

Por esta razón, toda empresa responsable por la seguridad de su información, debe asegurar la implementación de sistemas y modelos de seguridad para la protección de su información basados en estándares internacionales; esto también debe considerar al factor humano, pues tiene una gran importancia en

el éxito de la seguridad de la información. Tal es el caso del ICPNA Región Centro que en los últimos 15 años ha venido aumentando su interacción y manejo de información a través de tecnologías de la información en las ciudades donde tiene presencia, haciendo uso de redes internas y externas. Sin embargo, a pesar del aumento de su uso de tecnologías de la información, no se ha gestionado la seguridad de la información ni se ha fortalecido el factor humano en la empresa sobre este tema.

Por lo cual, a partir de una iniciativa del autor del estudio en coordinación con la Presidenta del Consejo Directivo, se decidió dar prioridad a un proyecto que se oriente a gestionar y generar cultura de la seguridad de la información a partir de algún estándar internacional. Con la aceptación del directorio y gerencias del ICPNA RC, se coordinó el recojo de información sobre conocimiento de seguridad de la información en el personal y sub gerentes del área de Tecnologías de la Información y las Telecomunicaciones y del área de Recursos Humanos. En resumen, general se encontró lo siguiente:

Tabla 1. Hallazgos de nivel de seguridad actual en la institución considerando descriptores de seguridad

	Descriptor de seguridad	Estado
1	Plan de gestión de seguridad de la información	Inexistente
2	Implementación del modelo de seguridad.	Inexistente
3	Identificación de activos críticos.	Nunca realizado
4	Identificación de vulnerabilidades	Nunca realizado
5	Implementación de controles.	Inexistente
6	Número de personas asignadas a la gestión de seguridad de la información (Mínimo 1).	Ninguna
7	Comité de seguridad de la información	Inexistente
8	Programa de gestión de incidentes de seguridad de la información	Inexistente
9	Existencia de políticas, normas, procedimientos e instructivos en procesos de información clave de la empresa	Inexistente
10	Numero de auditorías realizadas (Mínimo 1).	Ninguna
11	Número de capacitaciones sobre seguridad de la información hasta la fecha	Ninguna
12	Promedio de calificaciones de evaluaciones sobre conocimiento de seguridad de la información.	Nunca realizado
13	Tratamiento del personal para identificar comportamientos de riesgo en Seguridad de la Información.	Nunca realizado
14	Índice de satisfacción laboral en la empresa.	Nunca identificado

Esta información fue resumida de la información específica recogida en la institución debido al carácter confidencial de dicha información para la empresa; lo cual evidenció una necesidad inmediata de gestionar la seguridad de la información. El problema actual con respecto a la seguridad de la información en el ICPNA Región Centro involucra tanto a la parte de TI y el factor humano. Por consiguiente, a partir de esto, nace el problema de investigación.

1.1.2 Formulación del problema

A) Problema general

¿De qué forma se puede utilizar estándares y normativas de seguridad de la información dentro del ICPNA Región centro de modo que se fortalezca el factor humano dentro de un solo modelo orientado a proteger su información?

B) Problemas específicos

- ¿Cómo debe ser desarrollada una política de Seguridad de la información para proteger la información del ICPNA Región Centro?
- ¿Cómo puede concientizarse al personal y generar una cultura de seguridad de la información para proteger la información del ICPNA Región Centro?
- ¿Cómo puede gestionarse la seguridad de la información para proteger la información del ICPNA Región Centro de acuerdo a su realidad presente?

1.2 Objetivos

1.2.1 Objetivo general

Diseñar un modelo de seguridad de la información con un enfoque en el factor humano para proteger la información del ICPNA Región Centro.

1.2.2 Objetivos específicos

- Diseñar un modelo de política de Seguridad de la información para proteger la información del ICPNA Región Centro basado en estándares y normativa nacional e internacional.

- Diseñar un modelo de seguridad de la información que concientice al personal y genere una cultura de seguridad de la información para proteger la información del ICPNA Región Centro.
- Diseñar un modelo de seguridad de la información que gestione la seguridad de la información para proteger la información del ICPNA Región Centro de acuerdo a su realidad presente.

1.3 Justificación y delimitación

1.3.1 Justificación Académica

La elaboración del modelo de seguridad de la información con un enfoque en el factor humano permite ampliar los conocimientos sobre seguridad de la información, así como también permitirá consolidar y ampliar los conocimientos de gobierno y gestión de tecnologías de la información puesto que el modelo contempla áreas de manejo de personal con relación a la seguridad de la información. Además, es preciso mencionar que el producto final de este estudio permite profundizar en los aspectos humanos dentro de la seguridad de la información.

1.3.2 Justificación Científica

La investigación brinda una base de inicio a nuevos modelos de seguridad de la información o la mejora del mismo como un posible objeto de estudio científico que permita investigaciones futuras del tema tales como su aplicación en compañías de diversos tamaños, su aplicación en otros países con diversos trasfondos sociales y culturales o su adaptación en el contexto de seguridad actual a nivel global.

1.3.3 Justificación Tecnológica

Desde el punto de vista tecnológico, la investigación permite a las empresas gestionar la seguridad de su información considerando técnicas y procedimientos que los guíen a mejorar la seguridad de la información de sus empresas de forma eficiente. Además, este modelo provee herramientas de gestión que ayudan a reducir incidentes de seguridad de la información por falla del factor humano.

1.3.4 Delimitación

El estudio se llevó a cabo en un instituto dedicado a la enseñanza del idioma inglés denominado ICPNA Región Centro de la Ciudad de Huancayo en el año

2017 en un acuerdo entre el investigador y los directivos de dicha institución. Por lo cual su alcance es para el ámbito del ICPNA Región Centro de Huancayo.

1.4 Entregables del estudio y descripción de descriptores de seguridad de la información del modelo

1.4.1 Entregable general

El modelo de gestión de seguridad de la información con un enfoque en el factor humano para proteger la información del ICPNA Región Centro.

1.4.2 Entregables específicos

- Descripción y guía del modelo de seguridad de la información documentada.
- Formato de inventario de activos.
- Formato de matriz de riesgos.
- Modelo de política de seguridad de la información.
- Indicadores de evaluación del modelo

1.4.3 Descripción de descriptores de seguridad de la información para el modelo

Para poder evaluar el modelo de seguridad de la información se consideraron los siguientes indicadores cuyos valores mínimos dependerán de los criterios de la institución al momento de iniciar su gestión de seguridad de la información. Estos descriptores están basados en los 14 dominios de la ISO/IEC 27001:2013 (The International Organization for Standardization 2013) y fueron adaptados de la Guía de Indicadores de gestión para la seguridad de la información (MINTIC, 2015):

1.4.3.1 Plan de gestión de seguridad de la información:

Este indicador evalúa si se estableció o no un plan de seguridad de la información, lo cual da inicio a la gestión de seguridad de la información. Por lo cual se considera la existencia o inexistencia de este plan en los archivos de la empresa como valor de medición.

1.4.3.2 Implementación del modelo de seguridad

Este indicador considera el porcentaje de implementación del modelo de seguridad de la información dentro de la empresa, el porcentaje se determina considerando el número de fases del modelo implementadas dividido por el número de total de fases del modelo multiplicado por 100 para obtener el porcentaje de implementación.

1.4.3.3 Identificación de activos críticos

Este indicador permite identificar si se ha realizado un inventario de activos de seguridad de la información dentro de la empresa. Asimismo, permite controlar si se han identificado los activos críticos de la empresa para poder ser estudiados con respecto a sus vulnerabilidades y riesgos. El indicador se evalúa sobre la existencia o inexistencia del inventario procesado de activos críticos.

1.4.3.4 Identificación de vulnerabilidades y riesgos

La identificación de activos críticos no es suficiente; por lo cual es necesario identificar las vulnerabilidades y riesgos y considerar la existencia de una matriz de riesgos como resultado de dicha identificación. Por lo cual, el indicador de evaluación para esta área se mide por la existencia o inexistencia de dicha matriz.

1.4.3.5 Implementación de controles

La existencia de una matriz de riesgos que considera vulnerabilidades para los activos de información, no es suficiente para proteger la información; es necesario implementar controles para gestionar los riesgos dentro de la empresa. Por lo cual, es necesario realizar una identificación de controles para los riesgos encontrados. Sin embargo, el conocimiento de controles por cada riesgo no es suficiente para evaluar este aspecto de la gestión; es necesario considerar el porcentaje de implementación de estos controles. Para lo cual, se divide el número de controles implantados sobre el número total de controles identificados y se multiplica este resultado por 100.

1.4.3.6 Responsable y comité de seguridad de la información

Este indicador evalúa la formación y conformación del comité de seguridad de la información dentro de la empresa; lo cual comienza por la

designación del responsable de gestionar la seguridad de la información dentro de la institución. Por lo cual el valor de evaluación de este descriptor se determina por la existencia del personal de gestión de seguridad de la información considerando al menos el gestor de la seguridad de la información.

1.4.3.7 Programa de gestión de incidentes de seguridad de la información

Este indicador considera la gestión de incidentes de seguridad de la información. Para el caso de la implementación de la gestión de seguridad de la información se considera su existencia en la empresa. A partir de lo cual se pueden obtener sub indicadores de cumplimiento y gestión al analizar los incidentes registrados dentro de la su propia gestión; esto dependerá de la empresa y el alcance de su seguridad. Por lo cual, para el este estudio se considera la existencia o inexistencia de dicha gestión como indicador de cumplimiento necesario a partir de lo cual se pueden establecer otros indicadores que remplacen al de cumplimiento una vez establecida la gestión de incidentes.

1.4.3.8 Existencia de políticas, normas, procedimientos e instructivos en procesos de información clave de la empresa

Este indicador considera el árbol normativo dentro de la institución. Las políticas, normas, procedimientos e instructivos dentro de procesos clave en la empresa son documentos importantes y necesarios en la seguridad de la información. Por lo cual, el indicador sobre este punto se evalúa con respecto a su existencia o inexistencia en la empresa.

1.4.3.9 Auditorías realizadas

El número de auditorías de seguridad de la información realizadas en la empresa se considera un indicador necesario para evaluar la gestión de la gestión de la seguridad de la información. Por lo cual, se considera que 1 auditoria de seguridad de la información como mínimo es necesaria luego de un tiempo de implementar el modelo.

1.4.3.10 Capacitaciones sobre seguridad de la información

La capacitación sobre temas de seguridad de la información es necesaria dentro de la gestión de seguridad de la información; la generación de cultura y compartimiento de conocimiento de seguridad de la información

se basan en esto. Por lo cual, un indicador de evaluación de la gestión, sobre todo en el factor humano, es el número de capacitaciones realizadas sobre seguridad de la información.

1.4.3.11 Promedio de calificaciones de evaluaciones sobre conocimiento de seguridad de la información

Es necesario, además, considerar la evaluación periódica del conocimiento sobre temas de seguridad de la información en el personal de la empresa como un factor clave. Dicho promedio es un indicador de la madurez y tal conocimiento permite el compartimiento de información relacionada con la seguridad de la información, así como de la formación de cultura y comunidades de seguridad de la información. Además, es necesario considerar dicha calificación en la evaluación del personal realizada por el área de Recursos Humanos.

1.4.3.12 Tratamiento del personal para identificar comportamientos de riesgo en Seguridad de la Información.

Este indicador corresponde al estudio realizado como parte del modelo de gestión de seguridad de la información para identificar, por medio de un estudio psicológico, posibles comportamientos de riesgo de los trabajadores en la empresa. Este indicador se relaciona directamente a conocer al personal y dar tratamiento al factor humano de la seguridad de la información en la empresa. El indicador se evalúa sobre la base de si se realizó o no dicho tratamiento en el personal.

1.4.3.13 Índice de satisfacción laboral en la empresa

Este indicador se relaciona con el apoyo a la gestión de seguridad de la información de forma voluntaria. Aparte del establecimiento de las políticas de gobierno y gestión de seguridad de la información, se debe tener, si es posible, a todo el personal dispuesto a formar parte de la seguridad de la información. Para lo cual el nivel de satisfacción del personal es importante. La evaluación de este indicador se determina por el nivel de satisfacción laboral obtenido del estudio realizado para este propósito.

Todos estos indicadores son necesarios para evaluar el nivel de implementación y gestión de seguridad de la información. Sin, embargo, dependerá de la gestión del comité de seguridad y el alcance del plan de

seguridad de la información para determinar los porcentajes y números mínimos aceptables dentro de la empresa.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes de la investigación.

El artículo científico de (Safa, Von Solms y Furnell, 2016), que tiene como título "Information Security Policy Compliance Model in Organizations", cuyo objetivo fue de mejorar el comportamiento de seguridad de la información de los empleados en línea con las políticas y procedimientos de seguridad de la información, basados en involucramiento, apego, compromiso, y normas personales que derivan de la teoría de vínculos sociales. Plantea además que la seguridad de la información es una preocupación muy grande para los usuarios y las organizaciones debido a que la falta de conciencia, ignorancia, negligencia, apatía, mal manejo y resistencia sobre seguridad de la información es el principal causante de los errores que comenten los usuarios con respecto a la seguridad de la información.

El estudio se orientó a presentar un marco de trabajo conceptual que muestra como el cumplimiento de políticas de seguridad e información se lleva a cabo en las organizaciones. A partir de esto se creó un marco de referencia que muestra como los empleados cumplen las políticas de seguridad de la información organizacional. Los resultados de análisis de datos revelaron que compartir conocimiento seguridad de la información, colaboración, intervención, y experiencia tienen un efecto significativo sobre la actitud de los trabajadores hacia el cumplimiento de políticas de seguridad de la información organizacional. Sin embargo, el apego no tiene un efecto significativo sobre la actitud de los trabajadores hacia el cumplimiento de políticas de seguridad de la información. Además, los resultados muestran que el compromiso y las normas personales afectan la actitud de los trabajadores hacia el cumplimiento de políticas de seguridad de la información organizacional. Los factores identificados en los hallazgos

influencian en la actitud de los trabajadores hacia el cumplimiento de políticas y procedimientos de seguridad de la información organizacional y deben tenerse en cuenta si se desea fortalecer el factor humano de la seguridad de la información. El estudio revela el lado humano de la seguridad de la información y nos muestra aspectos aun no contemplados para poder fortalecer la seguridad de la información como complemento de los factores tecnológicos y documentarios que deben existir en una organización. Este trabajo aporta conocimientos comprobados en relación a factores que se deben tener en cuenta para poder fortalecer la seguridad de la información; además nos brinda un método para verificar la injerencia del factor humano la seguridad de la información y como el cumplimiento de políticas de seguridad de la información se puede mejorar al considerar características propias de los seres humanos.

El artículo científico de (Al-Mukahal y Alshare, 2015), que tiene como título “An examination of factors that influence the number of information security policy violations in Qatari organizations”, cuyo objetivo fue investigar los factores que impactan el número de violaciones de políticas de seguridad de la información en organizaciones de Qatari y examinar el moderado efecto de las dimensiones culturales de Hofstede en las relaciones entre factores independientes y el número de violaciones de políticas de seguridad de la información. Enfatiza que los sistemas de información se vuelven cada día más abiertos, distribuidos y expuestos; por consiguiente, tener un sistema de información fuertemente asegurado es una necesidad. A partir de esto, se han desarrollado muchos estudios sobre seguridad de la información en países desarrollados, pero no en países en vías de desarrollo. Para lo cual, fundado en teorías del área de criminología, sicología de comportamiento, y teoría de comportamiento planificado, dos componentes que afectan el número de violaciones de políticas de seguridad de la información fueron identificados. Un enfoque tentativo se usó al desarrollar un cuestionario para recolectar los datos. Los resultados muestran que la confianza, el impacto de implementar políticas de seguridad de la información en ambientes de trabajo y la claridad del enfoque de las políticas de seguridad de la información fueron factores significativos para predecir el número de violaciones de políticas de seguridad de la información. Los resultados demuestran que las dimensiones culturales como evasión y colectivismo de falta de certeza moderan las relaciones entre confianza, claridad de enfoque de políticas e impacto de políticas de seguridad de la información en el ambiente de trabajo y el número de violaciones de políticas de seguridad de la información. Este estudio muestra factores relacionados con el carácter humano para el éxito de las políticas de

seguridad de la seguridad de la información dentro de los ambientes de trabajo y evitar violaciones de políticas de seguridad de la información. Este estudio aportó con teorías, ideas e información que permitió establecer un modelo que consideró los factores mencionados u otros similares en el modelo de seguridad de la información que se propuso.

El artículo científico de (Safa y Von Solms, 2016), que tiene como título “An information security knowledge sharing model in organizations”, cuyo objetivo fue plantear un modelo que muestra cómo compartir el conocimiento de seguridad de la información pueden formar el riesgo de los incidentes de seguridad de la información. El mismo menciona que el tema de la seguridad de la información es aún un tema controversial para usuarios y compañías. El problema de como poder cuidar la integridad, confidencialidad y confiabilidad de la información en las empresas recae en sobre la conciencia de la seguridad de la información; sin embargo, son las personas las que deben tener esta conciencia; por lo tanto, el principal problema es cómo aumentar esta conciencia de la seguridad de la información. Para este estudio se utilizaron otros modelos de comportamiento humano como: La teoría de motivación, Teoría de comportamiento planeado y el Modelo de Triandi para poder conceptualizar la forma de compartir el conocimiento de seguridad de la información en las organizaciones. Se utilizaron enfoques cualitativos y cuantitativos para el desarrollo del modelo. Para comprender como la compartición del conocimiento se manifiesta en el contexto de seguridad de la información; se recolectaron los factores efectivos para compartir el conocimiento de seguridad de la información de una revisión de literatura; posteriormente, se desarrolló el modelo. Luego de esto, con la ayuda de expertos en la materia, se logró un segundo modelo final. Los resultados mostraron que ganarse una reputación, y ganarse una promoción como una motivación extrínseca y la satisfacción de la curiosidad como una motivación intrínseca tienen un efecto positivo en los empleados con respecto a compartir el conocimiento de seguridad de la información. Por otro lado, se encontró que la satisfacción de autoestima no influencia en la actitud de compartir el conocimiento de seguridad de la información. Además, los resultados revelaron que la actitud, control de comportamiento percibido y las normas subjetivas tienen un efecto positivo sobre la intención de compartir el conocimiento de seguridad de la información y que esta intención afecta el comportamiento. Asimismo, se evidencia que el apoyo organizacional influencia sobre la actitud de compartir el conocimiento de seguridad de la información más que la confianza. Se encontraron relaciones confirmatorias que integran diversos métodos teóricos del comportamiento humano para poder clarificar como compartir el

conocimiento de seguridad de la información. El compartir el conocimiento de seguridad de la información es un fenómeno importante; por lo tanto, las empresas deben establecer un ambiente apropiado en el cual cultivar esta cultura debido a sus ventajas. Además, la motivación es un factor vital para tener una actitud correcta hacia el comportamiento de compartir conocimiento de seguridad de la información. Del mismo modo, se demuestra que la motivación extrínseca tiene un más profundo efecto sobre la actitud. Por lo tanto, las empresas deben profundizar más en estos ámbitos. Este estudio muestra diversos factores que permiten que el compartir conocimiento de seguridad de la información sea más eficiente y por ende, se pueda mejorar el nivel de seguridad de la información con respecto al factor humano. Como factores determinantes se encuentra la motivación extrínseca y un ambiente adecuado donde fomentar la cultura de seguridad de la información. Este trabajo aporta con teorías y bases relevantes para la construcción de un modelo de gestión de seguridad de la información orientado al factor humano. Por último, brinda evidencia clave de como poder fortalecer el factor humano a través de variables específicas como la motivación externa.

El artículo científico de (Öğütçü, Testik y Chouseinoglou, 2016), que tiene como título “Analysis of personal information security behavior and awareness”, cuyo objetivo fue investigar los comportamientos arriesgados de los usuarios de los sistemas de información; así como las acciones preventivas de los usuarios, las amenazas a las cuales pueden estar expuestos, si tuvieran alguna experiencia adversa o a qué punto pueden percibir los riesgos. Este estudio plantea que los mecanismos de seguridad de software y el hardware son ampliamente usados para fortalecer los sistemas de información frente a los ataques. Sin embargo, estos sistemas son aun altamente vulnerables a las amenazas producidas por el comportamiento indeseado de los usuarios, el cual está cercanamente relacionado con la conciencia de seguridad de la información de los usuarios de los sistemas de información. Para lo cual, se desarrollaron cuatro escalas basadas en la data que se recolecto por medio de encuestas. Estas escalas son: Escala de comportamiento arriesgado, escala de comportamiento conservativo, escala de exposición a la ofensa y escala de percepción de riesgo. Las escalas desarrolladas a partir del contenido de las encuestas se aplicaron a alumnos, académicos, personal administrativo de una universidad en Turquía. De acuerdo a los resultados, cuantas más personas perciben amenazas, su comportamiento se vuelve más protector. Se encontró una relación positiva entre la escala de comportamiento conservativo y la escala la escala de percepción de riesgo. Además, existe una relación positiva entre la escala de

comportamiento arriesgado y la escala de exposición a la ofensa; debido a que cuando el uso de tecnologías riesgosas aumenta, aumenta también la probabilidad de estar expuesto al crimen o tener experiencias negativas; por supuesto, también aumenta su percepción al riesgo. Los resultados muestran que la más grande amenaza en los sistemas de información son los mismos usuarios de los sistemas de información, lo que significa que el eslabón más débil es el usuario humano. Además, lo que se vuelve importante y necesita ser asesorado es el comportamiento humano y los riesgos reales asociados. Las cuatro escalas desarrolladas muestran la relación que existe entre el conocimiento de seguridad de la información, la actitud de los usuarios ante el riesgo y la respuesta de estos usuarios ante situaciones de riesgos. Este estudio demuestra la importancia del factor humano y su tratamiento como factor de éxito de todo plan de seguridad de la información. El modelo y las cuatro escalas desarrolladas en este estudio sirven como base para considerar ciertos aspectos de comportamiento de usuarios para el modelo; por lo tanto, se consideró el estudio como un componente de consulta con respecto a los usuarios y el riesgo.

El artículo científico de (Safa, Solms y Futcher, 2016), que tiene como título “Human aspects of information security in organizations”, cuyo objetivo fue demostrar que mientras las personas son el eslabón más débil de la cadena de seguridad, a través de cooperación y coordinación, ellas pueden ser una fuente de fortaleza para desarrollar defensas eficientes. Este artículo establece que debido a que la información es el “core” de negocio de las organizaciones y empresas en la actualidad, y para poder proteger de forma satisfactoria este importante activo, los aspectos humanos, organizaciones y tecnológicos tiene un papel vital en la seguridad de la información. Los controles tecnológicos y organizacionales son críticos, pero ambos están relacionados con las personas. El problema radica en que al estar los controles tecnológicos y organizaciones relacionadas con las personas, se deben considerar un rango de aspectos humanos para proteger la información. Para el estudio se desarrolló un modelo basado en ciertos factores de éxito en la seguridad de la información como compartir el conocimiento de la seguridad de la información, colaboración en la seguridad de la información, comportamiento de cuidado consiente de la seguridad de la información, cumplimiento de políticas y procedimientos organizacionales de seguridad de la información y que se basan en las políticas de seguridad de la información. Se evidenció que el nivel de seguridad de la información depende de la manera en cómo se incluyan factores humanos como compartir el conocimiento de la seguridad de la información, colaboración en la seguridad de la información, comportamiento de cuidado consiente de la seguridad de la información, cumplimiento

de políticas y procedimientos organizacionales de seguridad de la información como factores que aseguran el éxito de todo plan de seguridad de la información. Basados en los resultados del estudio, se concluye que las técnicas y estudios actuales referidos a la seguridad de la información con base en el factor humano brindan un entendimiento importante a los académicos y a las personas que tienen que ver con las prácticas de seguridad de la información. El estudio describe de manera efectiva los componentes de un modelo que permite mejorar la seguridad de la información en las empresas. Este modelo brinda pilares que pueden ayudar a fomentar una cultura de seguridad de la información en las personas dentro de las empresas. Este estudio sirve como base teórica para el desarrollo del modelo de seguridad que se desea implementar porque brinda elementos actuales que se deben considerar en un plan de seguridad de la información con orientación al factor humano.

(Ampuero, 2011), realizó la tesis: “Diseño de un sistema de gestión de seguridad de información para una compañía de seguros”, en la Escuela de Pre Grado de la Pontificia Universidad Católica del Perú. El problema general del estudio se basa en incidentes de seguridad de la información a nivel mundial, donde se plantea una necesidad de poder implementar algún tipo de sistema que gestione la seguridad de la información para una compañía de seguros, puesto que en los últimos años se han presentado incidentes de seguridad en este tipo de empresas. A partir de esto se plantea el problema: ¿Cómo se puede gestionar la seguridad de la información de una compañía de seguros? El objetivo primordial del estudio fue desarrollar un sistema de gestión de seguridad de la información para una compañía de seguros. En el estudio, se utilizaron diversas metodologías como la norma AS/NZS 4360:2004 que es una metodología orientada para el tratamiento de riesgos de seguridad de la información; también se utilizó la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) para gestionar los riesgos; de estas 2 metodologías se tomó información para el sistema de gestión de seguridad de la información (SGSI). Asimismo, se utilizó la norma COBIT para los procedimientos y obtener información paso a paso de cómo gestionar el proceso de implementación del SGSI. Por último y de forma principal se utilizó el estándar ISO/IEC 27002:2005 para implementar el SGSI en la compañía de seguros. Como resultado de la tesis se implementó un sistema de gestión de seguridad de la información apropiada para una compañía de seguros; lo cual implica cualquier otro tipo de empresas aparte aquella donde se implementó este SGSI. Además, el estudio tiene las siguientes características:

- Se utilizó un estándar internacional, ISO/IEC 27002: 2005, para la implementación de un sistema de gestión de la seguridad de la información.
- Se hizo uso de otras metodologías para poder hacer una implementación del SGSI (Sistema de gestión de seguridad de la información) de forma más eficiente.
- Se logró identificar los riesgos, se realizó un plan de gestión de riesgos, y se creó la política de seguridad para la empresa.

Esta tesis propone la utilización de un estándar internacional como la ISO/IEC 27002: 2005 para poder gestionar la seguridad de una empresa. Además utiliza varios otros estándares y metodología que le permiten tener un sistema más robusto y que ayuda a la protección de los activos de la información. Esta tesis aporta con ideas y cuadros que se pueden referenciar en el modelo creado para identificar y gestionar los riesgos de seguridad de la información. Además nos brinda un modelo de aplicación de la ISO/IEC 27002: 2005 basados en el ciclo de calidad de Deming de mejora continua, lo cual se consideró también el modelo diseñado.

(Villena, 2010), realizó el estudio: “Sistema de gestión de seguridad de información para una institución financiera”, en la Escuela de Pre Grado de la Pontificia Universidad Católica del Perú. El estudio establece que el manejo de la seguridad de información en cada aspecto de una empresa es el principal problema si no se toma en consideración el adecuado tratamiento y control para los riesgos existentes. Por lo tanto, se requiere una administración efectiva desde una perspectiva de negocio considerando la normativa actual y no sólo dependiente de la tecnología. Este estudio tuvo como objetivo establecer los lineamientos principales para implementar un sistema de gestión de seguridad de información (SGSI) de forma adecuada en una institución financiera dentro del ámbito peruano. Esto con la finalidad de utilizar la tecnología de información y que esta se alinee a la estrategia de negocio de la empresa donde se implementará el SGSI considerando el valor de los activos y los riesgos implicados. Como parte de la metodología se utilizaron diversos estándares y metodologías de referencia como los modelos americanos de gobierno de tecnologías de la información (TI) para organizar los procesos dentro del área. Además, se hace uso de la normativa BS 7799 que brinda pautas para mejorar aspectos organizacionales, técnicos y de instalaciones; estas pautas sirven de dirección para la implementación de un sistema de seguridad de la información (SGSI), esta normativa también es conocida como la ISO 17799. También se utilizó la guía de buenas prácticas COBIT que está orientada a la gestión, auditoria de sistemas, control y seguridad. Esta guía establece que es lo que se debe implementar para tener una

estructura de control efectiva. Asimismo, se utilizó la normativa AS/NZS 4360:2004 como guía para la gestión de riesgos dentro de la empresa. Como resultado se obtuvo un sistema de gestión de seguridad de la información adecuado y específico para una institución financiera en general independiente de su tamaño en concordancia con las normas internacionales y nacionales como las de BASILEA II y la de la SBS que son indispensables para cualquier entidad financiera que quiera entrar al mercado. Además, el modelo tiene las siguientes características:

- Aporta pautas específicas de implementación de un SGSI
- Enfatiza la necesidad de promover una cultura de seguridad de la información dentro de las empresas.
- Detalla la documentación que se debe considerar en el modelo de SGSI.

Esta tesis tiene una perspectiva orientada al negocio, que en este caso es una institución financiera y que considera los aspectos técnicos, organizacionales y humanos para la implementación de un SGSI. Además, se hace uso de estándares de seguridad de la información adecuados y que permiten una gestión de la información y su seguridad eficiente. Además, la descripción sobre documentación que brinda es apropiada en relación a cómo debería otra institución financiera gestionar su seguridad de la información. Esta tesis aporta una perspectiva de implementación de un SGSI desde la óptica de negocios, en este caso, se utilizaron algunos aspectos de la tesis como las metodologías que usa y la forma como usa la documentación como referencia para poder crear el modelo de seguridad de la información que se diseñó para este estudio.

(Condori, 2012), realizó la investigación denominada: “Un Modelo de Evaluación de Factores Críticos de Éxito en la Implementación de la Seguridad en Sistemas de Información para determinar su influencia en la intención del usuario”, en la Escuela de Post Grado de la universidad Inca Garcilaso de la Vega. En la tesis se plantea el problema de investigación: ¿Cuál es el grado de influencia que ejercen los Factores Críticos de Éxito en la intención del usuario para la Implementación de Seguridad de Sistemas de Información en la Universidad Nacional del Altiplano-Puno durante el año 2011? La tesis tuvo como objetivo: determinar mediante un modelo estructural, el grado de influencia que ejercen los Factores Críticos de Éxito en la intención del usuario para la Implementación de Seguridad de Sistemas de Información en la Universidad Nacional del Altiplano Puno durante el año 2011. La investigación es de tipo explicativa porque determina las causas a un fenómeno específico, por medio del análisis que existe entre dos o más variables. Además, es de tipo transversal porque se buscó conocer que percepción tiene un usuario en una única oportunidad para

luego proceder a describir y analizar lo encontrado. Asimismo, se utiliza un diseño factorial debido a que se deseaba conocer en qué medida influencian los factores críticos de éxito identificados con referencia a la percepción de los usuarios de los diversos sistemas en la Universidad Nacional del Altiplano sin interferir con su interacción para conocer su comportamiento y percepción natural. Asimismo se utilizaron diversas teorías relacionadas con el comportamiento humano para poder identificar las intenciones de comportamiento para el estudio. En los resultados, considerando los factores de éxito identificados, se encontró que La Cultura Organizacional, los Recursos y Presupuesto, la Conciencia de la necesidad de seguridad por el personal contribuyen a la dimensión de Actitud para Implementar Seguridad en Sistemas de Información. Además, se muestra que el atributo con mayor importancia es Recursos y Presupuesto. Asimismo, se evidenció que el compromiso de la alta gerencia, la Misión de la Organización, la Formación y Capacitación, la Conciencia de la necesidad de seguridad por el personal, la Experiencia del usuario contribuyen a la dimensión del control conductual percibido. El factor con mayor importancia es la Formación y Capacitación. Además, el estudio tiene las siguientes características:

- En esta tesis se establecen nivel de correlación entre factores de éxito relacionados con aspectos organizaciones de la empresa donde se realizó el estudio
- Se muestra correlación entre factores relacionados con el área conductual de los trabajadores y el éxito de un sistema de gestión de seguridad de la información.
- Se hace énfasis en lo importante de factores como los recursos y el presupuesto y de la formación y capacitación para poder tener un sistema de gestión de seguridad de la información (SGSI) eficiente. Esto demuestra lo importante de la inversión en la seguridad de la información y las constantes capacitación que se deben tener con el personal.

Esta tesis demuestra la relación existente entre diversos factores de éxito para la implementación de un SGSI eficiente; entre los factores que considera de mayor relevancia se encuentran los de recursos y el presupuesto y de la formación y capacitación. Considerando los resultados, se puede observar que no sólo es cuestión de tecnología implementada en la organización, sino también de factores relacionados a la organización de la empresa con respecto a la seguridad de la información y factores humanos que tienen que ver con el comportamiento del personal. Esta tesis sirvió como referencia para comparar el modelo de seguridad que se diseñó; además se utilizaron criterios de esta tesis como referencia de los factores que se consideran

y como referente para establecer algunas secciones que se puedan homologar puesto que los factores mencionados, ya han sido demostrados como inherentes en la seguridad de la información.

(Talavera, 2013), realizó la tesis: “Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013”, en la Escuela de Pre Grado de la Pontificia Universidad Católica del Perú. La problemática se basa en la necesidad de los centros de salud de contar con un sistema de gestión de seguridad de la información que contemple las directivas de la Ley de datos personales de Perú (Ley 29733) que contempla un manejo adecuado de la información de índole personal de las personas y que debe contemplar un sistema de gestión de seguridad de la información (SGSI) para los centros de salud en el país. El objetivo de la tesis fue: Diseñar un sistema de gestión de seguridad de la información para una institución estatal de salud, de acuerdo a la norma ISO/IEC 27001:2013. La tesis hace usa como referencia principal la norma ISO/IEC 27001:2013 que se toma como base para establecer el SGSI. Además, se utiliza Business Process Management (BPM) para poder identificar y mapear los procesos de la organización de salud. Además, se usa la norma ISO/IEC 31000:2009 que brinda recomendaciones generales para la gestión de riesgos y contempla el plan de desarrollo de calidad de Deming; también se utiliza la norma ISO/IEC 27002:2013 como guía de implementación del SGSI. Por último, se utiliza la norma ISO/IEC 27799:2008 puesto que brinda especificaciones y especificaciones para considerar si se desea implementar un SGSI en una institución relacionada con el cuidado de la salud. El estudio dio como resultados el alcance del SGSI, y la política de seguridad de la información para la institución; además, se dio como entregable final el mapa de procesos de la institución de salud, la metodología de análisis de riesgos y de valoración de activos de la información. Por último, se concluye con la declaración de aplicabilidad de del SGSI basado en la norma ISO/IEC 27001:2013. Además, el estudio tiene las siguientes características:

- Se muestra un detallado proceso para la implementación de un SGSI
- Se brindan modelos y formatos para el inventario de activos, identificación de riesgos y la matriz de riesgos a implementar en un SGSI.
- Establece los lineamientos a considerar en el establecimiento de un SGSI para un centro de salud.

Esta tesis muestra de manera clara y especifica los pasos que se deben tener en cuenta para poder implementar un SGSI en una organización utilizando el ISO/IEC 27001:2013 como estándar base para la protección de la información dentro de una

empresa. Además, provee información relevante a la valoración de activos de la información y análisis de riesgo para poder implementar controles adecuados: por ultimo aporta con un modelo de política de seguridad de la información adecuada para la institución de referencia. Para el caso del modelo de seguridad de la información que se diseñó, la tesis propuesta aportó con formatos e ideas a considera para poder generar formatos relacionados a los activos de la información y los riesgos que se deben de considerar en la gestión de riesgos. Además, brida ideas para gestionar la seguridad en organizaciones tal como el modelo diseñado.

(Reyes, 2011), realizó el estudio: “Un Modelo de Evaluación de Factores Críticos de Éxito en la Implementación de la Seguridad en Sistemas de Información para determinar su influencia en la intención del usuario”, en la Escuela de Pre Grado de la Universidad Nacional Autónoma de México. La investigación estipula que, con los avances de las tecnologías de la información y las comunicaciones, se hace necesario conocer el rumbo que debe tomar la seguridad informática en el mundo para planear la formación de recursos humanos altamente capacitados para afrontar los retos que estos avances traen a futuro. Es pues la problemática el conocer que se puede hacer para afrontar los retos de la seguridad de la información. La investigación tuvo como propósito realizar una investigación que permita estudiar, analizar y determinar la situación actual de la seguridad informática en México y su contraste a nivel internacional. Para este estudio se utilizó un método descriptivo que se basó en investigación literaria adecuada para para generar un modelo educativo con respecto a la seguridad de la información. Este modelo contempla diversos temas específicos y actuales en temas de seguridad de la información para todo el sector educativo desde primaria hasta educación superior con la finalidad de tener personas conocedoras de los fundamentos de seguridad de la información. Como resultados de la investigación se obtuvieron, un modelo educativo dividido por estratos educativos que contempla en todos los casos la creación y crecimiento de una cultura de seguridad de la información en todos los involucrados. Además, se da como resultado el currículum, el temario y el desarrollo de todos elementos de seguridad de la información relevantes para el ámbito actual. Además, la tesis tiene las siguientes características:

- Se muestran aspectos de la seguridad de la información relevantes a la actualidad.
- Se presentan aspectos metodológicos para poder generar una cultura de seguridad de la información en estudiantes.

Se describe con claridad cada uno de los componentes y especificaciones de seguridad de la información con respecto a prevención y auditoria de sistemas.
La tesis describe de manera clara y precisa diversos conceptos que van acorde con la cultura de seguridad de la información; además, se establece un modelo curricular para la educación de estudiantes en diversos niveles educativos partiendo desde primaria hasta educación superior. Este trabajo aportó con algunas pautas necesarias para el área de educación en temas de seguridad de la información en el personal de las empresas donde se desee implementar el modelo de seguridad de la información que se desarrolla: además, provee información relevante para generar cultura de seguridad de la información dentro de las empresas. Esto es clave para trabajar el factor humano de la seguridad que el modelo diseñado contempla.

El trabajo de (Spitzner, 2016) sobre el factor humano en la seguridad de la información titulado: “Securing the Human to be Mightier than the Computer,” nos menciona que la gente y no la tecnología se están volviendo la clave para asegurar las organizaciones hoy en día. Por años, las organizaciones han invertido en tecnología como antivirus, firewalls, encriptación completa de discos, o prevención de perdida de información. Sin embargo, todas estas y otras herramientas fallan en asegurar un elemento clave, las personas. El problema más grave que tiene la seguridad de la información son las personas y mientras que las organizaciones no enfoquen el elemento humano, los incidentes de seguridad continuarán afectando las empresas. Las empresas invierten tecnología, pero también deberían invertir en asegurar a las personas, y para esto se necesita asegurar el comportamiento de las personas. Además, los ataques informáticos y las fallas de seguridad vienen en su mayoría del área humana de las empresas por ser el punto más débil de la organización; y lo hacen por medio de convencer a los trabajadores a hacer cosas que no deberían hacer. Para esto, el primer paso es crear un programa de conciencia de seguridad que se les quede a los trabajadores; para esto se debe comprender como es que el comportamiento se modifica y esto empieza en muchos casos por motivar a las personas hacia un cambio en el trabajo y a nivel personal. En segundo lugar, se debe comunicar el mensaje con un método que la gente comprenda bien y que las capacitaciones tengan impacto, considerando sus emociones. Por último, es importante valorar a aquellos que demuestran el comportamiento adecuado porque el reconocimiento es un factor vital de motivación. Como conclusión se menciona que la gente es la mejor defensa que una organización puede tener; desafortunadamente, también son el área más descuidada. Por último, si se invierte en tecnología también se debería invertir en los empleados, puesto que esto traerá beneficios no sólo para

las empresas sino para las personas mismas. El artículo, muestra de manera clara y precisa la necesidad de invertir en el factor humano de las organizaciones como parte de una estrategia para fortalecer la seguridad de las organizaciones y de sus trabajadores como individuos. Además, se brindan algunos consejos que considerar para fortalecer la seguridad de la información. Este articulo aporta ideas practicas a tomar en cuenta para el desarrollo del modelo seguridad de la información que se desea elaborar; es por lo tanto un referente de sugerencias que se consideró para la investigación realizada.

De la entrevista con (Valdivia, 2016), quien cuenta con certificaciones: CISA, CISM, CCISO, ITILv3 and CI-SCS y es conocedor del tema de seguridad de la información con una experiencia de 18 años, mencionó que el factor humano es uno de los grandes problemas que comprometen la información de las compañías; esto se confirma por estudios que indican que el problema son precisamente los usuarios de los sistemas de información y las amenazas internas; entonces, un proyecto de tesis que apoye a resolver el problema del comportamiento de los usuarios, del factor humano dentro de las compañías, es de suma relevancia. Además, sugirió establecer un modelo que podría ser basado en el componente humano, u componente de la ISO 27002, y algunas prácticas de seguridad para elaborar un modelo que sea aplicable a la realidad peruana. Recomendó utilizar la ISO antes que la norma técnica peruana en temas de seguridad de la información debido a su alcance normativo y aplicativo. Del mismo modo, recomendó que el marco teórico debería tener temas de comportamiento de usuarios relacionados con la seguridad de la información como base del modelo; esto se debe a que los si bien es cierto, los ataques más sonados en los medios de comunicación son los ataques externos, pero la realidad, y menciono con base a su experiencia personal diaria, es que el problema son los usuarios internos, la gente que tiene acceso a la información, enfatizando que ahí está la verdadera amenaza. Por lo tanto, se debería considerar temas que ayuden a mejorar el comportamiento humano. El experto al que se entrevistó confirma la realidad presente que artículos científicos actuales abordan en sus temas de investigación; además su opinión contribuyó con información sobre lo que debería contener el marco teórico de la tesis sobre el comportamiento humano y su relación con la seguridad de la información.

2.2 Bases teóricas

2.2.1 Fundamentos teóricos

Para la elaboración del modelo de seguridad de la información, debido a que se orientó al fortalecimiento del factor humano, fue necesario considerar teorías relacionadas al comportamiento humano, individual y colectivo; por eso, en esta sección se consideraron teorías psicológicas y sociológicas de comportamiento humano que fueron sugeridas de forma indirecta por los estudios presentados en el capítulo I en la sección de antecedentes. Estas teorías permitieron establecer estrategias que ayudaron al fortalecimiento del factor humano en el modelo de seguridad de la información que fue elaborado.

2.2.1.1 Teoría de las necesidades básicas

Feist (2007) realizó un estudio sobre la teoría de motivación de Maslow y las necesidades básicas en la vida de los seres humanos; entre las ideas que él plantea, se establecen criterios demostrados por medio de observación in situ donde se evidencia el orden de cómo se satisfacen las necesidades humanas. Sin embargo, Maslow también pudo evidenciar que estas necesidades tenían también cierto grado de complejidad debido a que no siempre cumplían el orden que se estableció en su teoría; partiendo de esta premisa, pudo observar que la autorrealización es el fin de las necesidades humanas y que existen ciertos rasgos característicos que impulsan a una persona a buscar la autorrealización; entre ellos establece valores; una percepción más eficiente de la realidad; aceptación de sí mismo, de los demás y la naturaleza; espontaneidad, sencillez y naturalidad; interés por los problemas más allá de sí mismos; necesidad de intimidad, Autonomía; apreciación permanente de las cosas buenas de la vida; la experiencia cumbre; espíritu comunitario; relaciones interpersonales profundas; carácter democrático; distinción entre medios y fines; sentido del humor filosófico; creatividad y resistencia a las convenciones sociales. A continuación, se describe más a detalle cada una de las necesidades descritas por Maslow.

2.2.1.1.1 Necesidades fisiológicas

Estas son las necesidades más elementales dentro de la descripción de necesidades propuestas por Maslow; “Las necesidades más básicas de cualquier persona son las necesidades fisiológicas, entre

ellas el alimento, el agua, el oxígeno, la temperatura corporal, etc. Las necesidades fisiológicas prevalecen por encima de todas las demás" (Feist, 2007, p. 277). "También son llamadas necesidades biológicas y son las de alimentación, bebida, refugio, sexo, protección contra el dolor, etc." (Arbaiza Fermini, 2010, p. 154).

2.2.1.1.2 Necesidades de seguridad y estabilidad

Luego de cubiertas las necesidades esenciales se establecen las de seguridad y estabilidad; estas necesidades "incluyen seguridad física, estabilidad, dependencia, libertad y protección de fuerza amenazadoras como la guerra, el terrorismo, la enfermedad, el miedo, la ansiedad, el peligro, el caos y los desastres naturales"…"Las necesidades de seguridad difieren de las necesidades fisiológicas en que no se pueden satisfacer en exceso" (Feist, 2007 p.p. 277). "Son las necesidades de estar libres de amenaza y protección contra los daños físicos y emocionales" (Arbaiza Fermini, 2010, p. 154).

2.2.1.1.3 Necesidades sociales y de afiliación

Este grupo de necesidades sale fuera de nuestro círculo personal y contempla aspectos "…como el deseo de amistad, el deseo de tener una pareja e hijos, la necesidad de pertenecer a una familia, un club, un barrio, una nación. Estas necesidades incluyen también algunos aspectos de contacto sexual y humano, así como la necesidad de dar y recibir amor. (Maslow, 1970)." (Feist, 2007 p.p. 278). En otras palabras, "son el afecto, el sentido de afiliación y pertenencia, amistad e interacción" (Arbaiza Fermini, 2010, p. 154).

2.2.1.1.4 Necesidades de estima y reconocimiento

En las necesidades de estima y reconocimiento se "incluyen el amor propio, la confianza, la competencia y la percepción de aprecio de los demás. Maslow (1970) identificó dos niveles de necesidades de respeto: la reputación y la autoestima" (Feist, 2007 p.p. 278). Es decir, "son el amor propio, la auto-confianza, el status, el reconocimiento, etc." (Arbaiza Fermini, 2010, p. 155).

2.2.1.1.5 Necesidades de autorrealización

Este es el grupo más elevado de necesidades y “Abarcan el logro personal, la realización de potencial de la persona, y un deseo de creatividad en toda la extensión de la palabra (Maslow, 1970). Las personas que han alcanzado el nivel de autorrealización se hacen seres humanos plenos y logran satisfacer necesidades que otros sólo vislumbran o nunca llegan a percibir” (Feist, 2007 p.p. 279). Por lo tanto, “son las más elevadas del ser humano y reflejan el esfuerzo de una persona por alcanzar su máximo potencial y crecimiento” (Arbaiza Fermini, 2010, p. 155).

2.2.1.2 Teoría del comportamiento planificado

En 1991, Ajzen propuso su teoría de comportamiento planificado (TCP) donde estipulaba que la conducta individual podía ser predicha por las intenciones del mismo individuo; mientras que las intenciones son predichas por las actitudes acerca del comportamiento, las normas subjetivas (son la percepción de una persona sobre las creencias importantes de otros que debería o no hacer) que motiva la ejecución del comportamiento y la percepción individual de su control sobre el comportamiento. Esta teoría ha sido usada para predecir comportamientos en una variedad de individuos y situaciones (Cameron, 2012). La TCP describe que “Las actitudes sociales surgen de la interacción entre las expectativas conductuales y su valoración por parte de cada sujeto, en tanto que la norma subjetiva sería el modo en que el sujeto recibe e interpreta lo que dicen las personas y los grupos que considera relevantes acerca de lo que debería hacer en relación con la conducta y la motivación para acomodarse a estas opiniones, mientras que el control conductual percibido contiene las creencias que poseen los sujetos sobre su propia capacidad para realizar una conducta determinada” (Martín, Manuel y Rojas, 2011, p. 434).

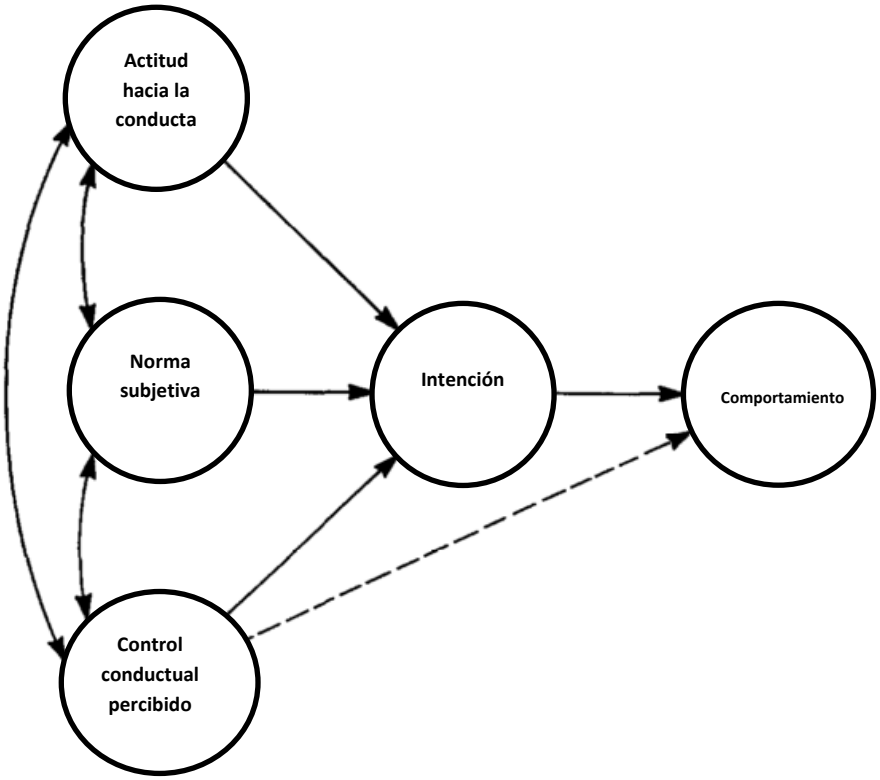

Figura 7: Teoría del comportamiento planificado.

Fuente: (Ajzen, 1991)

2.2.1.2.1 Control conductual percibido

Este es un componente importante de la teoría del control planificado debido a que los recursos y las oportunidades que tiene una persona, deben dictar hasta cierto punto, la probabilidad de logro conductual. Este se percibe como cuan fácil o difícil de realizar es un comportamiento. Se debe considerar la percepción de control conductual y su impacto en las intenciones y las acciones. El control conductual percibido sumado a una intensión conductual pueden ser usados para predecir la probabilidad de un intento conductual exitoso (Ajzen, 1991).

2.2.1.2.2 Norma subjetiva

Las normas subjetivas se basan en la premisa de que existe la probabilidad de que individuos de referencia importantes aprueben o desaprueben la ocurrencia de un comportamiento dado. Del mismo modo, un comportamiento puede ser influenciado también por las normas morales o personales del individuo que muestran obligación o

responsabilidad moral con respecto a realizar o rechazar un determinado comportamiento (Ajzen, 1991).

2.2.1.2.3 Actitud hacia la conducta

Se refiere al grado en que una persona tiene una evaluación o aprecio favorable o desfavorable de un comportamiento en cuestión. En otras palabras, tendemos a evaluar como positivo o negativo cierto comportamiento dependiendo de la circunstancia. De esta manera, aprendemos a favorecer lo que nosotros creemos que tiene consecuencias realmente deseables y nos formamos actitudes no favorables hacia comportamientos que asociamos con consecuencias generalmente indeseables; el valor de la consecuencia contribuye a la actitud en proporción directa a la fuerza de la creencia (Ajzen, 1991).

2.2.1.3 Teoría de control social

La teoría de control social hace referencia a que las actividades delictivas se originan de rupturas o debilitaciones de la relación individuo-sociedad (Hirschi, 2003). “Mientras más débiles sean los grupos a los cuales pertenezca [el individuo], menos dependerá él de ellos; por consiguiente, el individuo dependerá más de sí mismo y no reconocerá otras reglas de conducta que no se basen en sus intereses particulares (Durkheim, 1951)” (Hirschi, 2003, p. 8). De donde se entiende que “El control social puede entenderse como el conjunto de instrumentos (generalmente normativos), instituciones y acciones encaminadas al cumplimiento de los fines y valores propuestos por el sistema imperante, logrando en esta forma mantener el orden social” (López, 2014, p. 7). “Las teorías que se engloban dentro del control social, tratan de comprender y explicar cuáles son los factores o fuerzas que obligan a la mayoría de las personas, la mayor parte del tiempo a comportarse de forma no criminal aún en presencia de oportunidad.” (López, 2014, p. 6). En resumen, sin un control social adecuado, se ayudará y fomentarán los comportamientos no deseados. Según (Hirschi, 2003) existen cuatro elementos que conforman el vínculo de control social.

2.2.1.3.1 El apego

Según la sociología, el hombre es sensible a la opinión de los demás, por eso, una conducta anómala no es considerada aceptable. De donde “violar una norma es actuar de modo contrario a los deseos y expectativas de las demás personas. Si a una persona no le importan ni los deseos ni las expectativas de las demás personas, es decir, que es insensible a la opinión de los demás, en esa medida, por lo tanto, no se hallará sujeta a las normas. Es libre para desviarse.” (Hirschi, 2003, p. 11). El apego a los demás (familia, amigos, colegas, sociedad) permite que se acepten ciertas normas de conducta que ayuden a evitar actitudes y comportamientos no deseados.

2.2.1.3.2 El compromiso

“Pocos podrían negar que los hombres obedecen de cuando en cuando las reglas por el simple hecho de temer a las consecuencias. Este componente racional de la conformidad lo denominamos compromiso” (Hirschi, 2003, p. 12). Esta forma de actuar que involucra energía, tiempo y a uno mismo considera las consecuencias y el riesgo de tener actitudes desviadas y sus posibles consecuencias; esto a partir de una evaluación de las consecuencias que podría generar dicha conducta. Esto hace suponer que una sociedad organizada no pondrá en riesgos sus propios intereses por querer cometer actos delictivos debido a que no quiere perder lo que obtiene con esfuerzo (Hirschi, 2003).

2.2.1.3.3 La participación

La idea de participación conlleva en sí misma la naturaleza del tiempo y de lo que podemos hacer en un limitado número de horas al día; es decir, aunque queramos ser y hacer muchas cosas en nuestra vida, no podremos hacer mucho de lo que quisiéramos debido a que el tiempo para hacer todo eso es muy limitado. Incluso si se deseara realizar acciones ilícitas, se tendría que dejar de lado muchas otras actividades para poder hacerlas. “Sin duda alguna, muchas personas le deben una vida virtuosa a una falta de oportunidad de hacer lo contrario. El tiempo y la energía son limitados por naturaleza” (Hirschi, 2003, p. 15). Por lo tanto, el estar ocupado en actividades comunes y convencionales, definitivamente constituye un elemento de la teoría

de control. “La presunción, ampliamente compartida, es que una persona sencillamente se puede hallar tan ocupada en sus asuntos convencionales como para no encontrar el tiempo necesario para comprometerse en una conducta desviada” (Hirschi, 2003, p. 15).

2.2.1.3.4 Las creencias

La teoría de control presupone la existencia de un conjunto de normas morales que existen en la sociedad y que, si alguien no está viviendo en estas normas, es porque tiene sus propias normas de conducta y que su accionar está dentro de lo que cree. Sin embargo, si una persona cree en las normas de la sociedad, se tendría que explicar porque quebranta las normas en las que cree. “En otras palabras, no sólo suponemos que el desviado ha creído en dichas reglas, sino que suponemos que él cree en las reglas aun cuando las viola” (Hirschi, 2003, p. 16). Esto haya explicación si aquel que quebranta las reglas, no cree realmente en ellas, aunque las conozca y estas sean meras palabras; o también si la persona evalúa que él puede quebrantar la norma, pero al mismo tiempo creer en ella. “La idea de un sistema de valores comunes (o quizás mejor, un sólo sistema de valores) es coherente con el hecho, o presunción, de la variación de la intensidad de las creencias morales” (Hirschi, 2003, p. 20).

2.2.2 Metodologías existentes

Para poder salvaguardar la seguridad de la información en una empresa, existen diversas normas y estándares que permiten gestionar la seguridad de la información. Para el caso del modelo de seguridad de la información, se utilizaron como referencia normas como ISO/IEC 27002: 2013, MAGERIT V.3 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), la Norma Técnica Peruana NTP-ISO/IEC 27001 – 2014 y la Ley de Protección de Datos Personales (Ley 29733) con el siguiente propósito:

- ISO/IEC 27002: 2013, se utilizó con el propósito de revisar la gestión de seguridad de la información y las buenas prácticas de este estándar. Del mismo modo, la distribución de sus dominios y controles sirvió como base para sugerir la política de seguridad de la información dentro del modelo elaborado.

- MAGERIT V.3, se utilizó para la parte de gestión de riesgos del modelo, así como la elaboración de plantillas de inventario de activos, la matriz de riesgos y la matriz de controles. Del mismo modo se consideró esta metodología para la evaluación de vulnerabilidades para la gestión de riesgos.
- La Norma Técnica Peruana NTP-ISO/IEC 27001 – 2014, fue utilizada como referencia de seguridad de la información relevante a la realidad peruana. Esta norma concuerda con la ISO/IEC 27002: 2013, pues se basó en ella, pero para el modelo, sirvió como referencia debido a ser una norma aplicable en nuestro país.
- Ley de Protección de Datos Personales (Ley 29733), se utilizó puesto que la protección de datos personales debe considerarse en la gestión de seguridad de la información. Esta ley y su normativa se encuentran alineadas con la NTP-ISO/IEC 27001 – 2014 y se consideró en la elaboración del modelo y la protección de datos personales dentro de la institución.

A continuación, se procede a describir cada una de los estándares y normativas utilizadas.

2.2.2.1 ISO/IEC 27002: 2013

El estándar ISO/IEC 27002 es parte de la familia ISO/IEC 27000 y que contiene la descripción de los controles que se deben implementar para obtener la certificación ISO 27001. Está norma está dividida 14 dominios, 35 objetivos de control y 114 controles (ISO27000.es, 2016). Este estándar internacional contiene una lista de objetivos de control comúnmente aceptados y controles de mejores prácticas para ser usadas como una guía de implementación cuando se seleccionan e implementan controles para lograr la seguridad de la información (The International Organization for Standardization, 2016). Los catorce dominios del estándar se mencionan a continuación, pero se describen en su contenido en el ANEXO 1:

- Políticas de seguridad
- Aspectos organizativos de la seguridad de la información
- Seguridad ligada a los recursos humanos
- Gestión de activos

- Control de accesos
- Cifrado
- Seguridad física y ambiental
- Seguridad operativa
- Seguridad en las telecomunicaciones
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Relaciones con proveedores
- Gestión de incidentes en la seguridad de la información
- Aspectos de la seguridad de la información en la gestión de la continuidad del negocio.
- Cumplimiento

2.2.2.2 MAGERIT V.3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

El portal web de administración electrónica de España brinda una definición acerca de MAGERIT (Amutio Gómez, 2012):

> MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.
>
> La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.
>
> MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

MAGERIT persigue los siguientes objetivos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso (Consejo Superior de Administración Electrónica 2016).

2.2.2.3 Norma Técnica Peruana NTP-ISO/IEC 27001 – 2014

Esta norma fue desarrollada por el Comité Técnico de Normalización de Codificación e intercambio electrónico de datos y oficializada el 01 de diciembre de 2014 basada en diversos estándares internacionales (ISO) relacionados a la seguridad de la información y la gestión de riesgos. En dicho proyecto participaron diversas instituciones como B2IMPROVE S.A.C, Deloitte & Touche S.R.L., DMS Perú S.A.C. INDECOPI, NSF INASSA SAC., Superintendencia de Administración Tributaria – SUNAT, GS1 PERU, Contraloría General de la República, FOLIUM S.A.C., ONGEI, entre otros consultores externos expertos en la materia.

La NTP-ISO/IEC 27001 – 2014 se elaboró con la finalidad de brindar “requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información.” (INDECOPI, 2014). Asimismo, la norma brinda requisitos genéricos necesarios para la gestión de riesgos de seguridad de la información dentro de una organización. Por lo cual se considera una decisión acertada y necesaria la implementación de un sistema de gestión de seguridad de la información según la óptica de la norma Peruana.

2.2.2.4 Ley de Protección de Datos Personales (Ley 29733)

La Ley de Protección de Datos Personales, ley 29733, fue promulgada el 11 de julio de 2011 y su reglamento fue publicado el 22 de marzo de 2013. Esta ley "tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen." (Congreso de la República del Perú, 2011). Esta ley y su reglamento se enfocan en el tratamiento de datos personales en las entidades de orden público e instituciones privadas y cuya aplicación es de carácter obligatorio.

2.2.3 Técnicas e instrumentos de investigación

Para la realización del modelo de seguridad de la información se necesitó como instrumento principal la recolección de información relacionada a la seguridad de la información y su relación con el factor humano dentro de las empresas. Para esto se hizo uso de fuentes de información primarias; esta información fue necesaria para conocer cómo se está manejando el tema de la seguridad de la información en las empresas a nivel mundial y que guías, estándares y procedimientos existen en la materia, así también, conocer las iniciativas de solución ante el problema del factor humano en la seguridad de la información como punto débil; además, para conocer la realidad del ICPNA Región Centro en temas de seguridad de la información, se hizo uso de la observación directa y de entrevistas con personal administrativo y docente en el ICPNA Región Centro y con expertos en la materia para poder obtener información relevante para desarrollar el modelo.

2.2.4 Diseño de modelo teórico conceptual

En base a la información de los antecedentes, que consideran el factor humano como el punto más frágil de la seguridad de la información, las teorías de comportamiento, que son mencionadas en los antecedentes como parte de fortalecimiento individual del factor humano en casos individuales y los estándares internacionales junto a la normativa vigente sobre seguridad de la información, se procedió a diseñar el modelo teórico conceptual para el desarrollo del modelo de seguridad de la información.

En primer lugar, se consideró para la elaboración del modelo de seguridad de la información la teoría de necesidades básicas considerando el nivel de satisfacción personal e institucional basada en la satisfacción de sus necesidades personales como base para generar la cultura de seguridad de la información. Además, se consideró la teoría de comportamiento planificado con respecto a la identificación de patrones de conducta orientadas a la seguridad de la información que se puedan modificar con orientación del modelo y con apoyo del área de RRHH en la institución. Así también, se consideró la teoría de control social en el modelo para poder fomentar el compartimiento de conocimiento de seguridad de la información y la generación y fortalecimiento de la cultura de seguridad de la información.

Del mismo modo, para la elaboración del modelo, también se consideraron como base los estándares como ISO/IEC 27002: 2013, MAGERIT V.3, la Norma Técnica Peruana NTP-ISO/IEC 27001 – 2014 y la Ley 29733 como referencia para el establecimiento del modelo como se describió en el acápite 2.2.2. Asimismo, se utilizó la información sobre el nivel de seguridad de la información recopilada del ICPNA Región Centro para poder considerar la aplicabilidad del modelo de seguridad de la información. El modelo de seguridad de la información se orienta a la gestión de seguridad de la información y al fortalecimiento del factor humano que es el objetivo del modelo. La figura 8 ilustra el modelo teórico conceptual

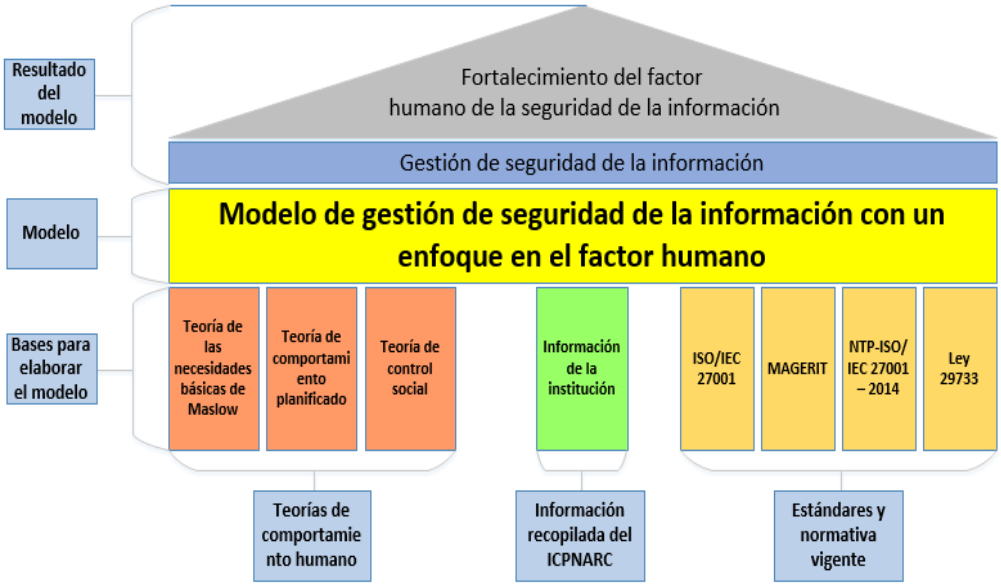

Figura 8: Modelo teórico conceptual del modelo de seguridad de la información. Fuente: (Elaboración propia)

2.3 Definición de términos básicos

A continuación, se listan términos básicos necesarios para comprender el modelo de seguridad de la información:

Actitud

"Tendencia o predisposición relativamente duradera para evaluar de un determinado modo a una persona, suceso o situación a partir de los significados que se les da y a actuar en consonancia con esta evaluación" (Consuegra Anaya, 2010).

Activo

"(Inglés: Asset). En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización" (The International Organization for Standardization, 2016).

Amenaza

"(Inglés: Threat). Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización" (The International Organization for Standardization, 2016).

Árbol normativo

Conjunto de documento que contienen políticas, procedimientos, instructivos y registros.

Conciencia de seguridad de la información

Se define como la "facilidad para pensar habitualmente, en como eliminar riesgos de seguridad de la información producto del trabajo que se encuentran presentes en las tareas que normalmente realizamos" (The International Organization for Standardization, 2016).

Confidencialidad

"(Inglés: Confidentiality). Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados" (The International Organization for Standardization, 2016).

Conducta / Comportamiento

"Reacción global del sujeto frente a las diferentes situaciones. Toda conducta es una comunicación, que a su vez no puede sino provocar una respuesta, que

consiste en otra conducta-comunicación. / Respuesta o acto observable o mensurable" (Consuegra Anaya, 2010).

Control

"Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo" (The International Organization for Standardization, 2016).

Cultura de la seguridad de la información

"La Cultura de Seguridad es la combinación de los valores, actitudes, competencias y modos de comportamiento, tanto individuales como de grupo, que determinan el compromiso, modelo y competencia de la gestión de la seguridad en la organización (The International Organization for Standardization, 2016).

Datos sensibles

"Es aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales, la información relativa a la salud física o mental u otras análogas que afecten su intimidad" (Gobierno/Perú, 2012).

Disponibilidad

"(Inglés: Availability). Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada" (The International Organization for Standardization, 2016).

Incidente de seguridad de la información

"(Inglés: Information security incident). Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información" (The International Organization for Standardization, 2016).

Ingeniería social

Conjunto de técnicas que a través del engaño obtienen información de una empresa directamente de los trabajadores.

Integridad

“(Inglés: Integrity). Propiedad de la información relativa a su exactitud y completitud” (The International Organization for Standardization, 2016).

Malware / software malicioso

Software dañino, existen virus, troyanos, gusanos, etc.

Mejora continua

Concepto planteado por Deming en su modelo de calidad para negocios para la mejora continua.

Política de seguridad de la información

“Documento de que contiene políticas o normas relacionadas con la seguridad de la información y son de ejecución obligatoria” (The International Organization for Standardization, 2016).

Riesgo

“(Inglés: Risk). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias” (The International Organization for Standardization, 2016).

Segregación de funciones

“(Inglés: Segregation of duties). Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia” (The International Organization for Standardization, 2016).

Seguridad de la información

“(Inglés: Information security). Preservación de la confidencialidad, integridad y disponibilidad de la información” (The International Organization for Standardization, 2016).

Stakeholder

“(Inglés: Interested party / Stakeholder). Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una

decisión o actividad” (The International Organization for Standardization, 2016).

Vulnerabilidad

“(Inglés: Vulnerability). Debilidad de un activo o control que puede ser explotada por una o más amenazas” (The International Organization for Standardization, 2016).

CAPÍTULO III

METODOLOGÍA

3.1 Método y alcances de la investigación

3.1.1 Método de la investigación

Para la elaboración del modelo de seguridad de la información, se hizo uso de métodos generales y específicos que permitieron comprender la situación de seguridad de información del ICPNA Región Centro y la gestión que se le da a la seguridad de la información según estándares internacionales. De este modo, se logró diseñar el modelo de seguridad información que considera el fortalecimiento del factor humano como valor adicional del modelo.

A) Método general o teórico de la investigación

Para la investigación se utilizó el siguiente método:

- **Método analítico-sintético:** Para evaluar la situación de la seguridad de la información del ICPNA Región Centro en un nivel especifico y general de forma holística y sistémica se utilizó este método debido a que “una empresa es concebida como un sistema abierto, dinámico y complejo” (Rojas Rodríguez y Aguilar Marín, 2013), tal cual es el caso del ICPNA Región Centro. Además, se utilizó este método para determinar los componentes de seguridad de la información presentes y sus relaciones entre sí dentro de la empresa para luego utilizar los componentes teóricos presentados y formular el modelo de seguridad de la información de modo que cubra cada aspecto de la gestión de seguridad de la información en la institución.

B) Método específico de la investigación

Para la investigación se utilizaron los siguientes métodos:

- **Ciclo de la calidad de Deming:** Este ciclo de calidad se utilizó como parte de la mejora continua del modelo de seguridad de la información a implementar.
- **Método de diseño de modelo:** Este método específico ayudó a formar el modelo de seguridad de la información en su estructura y forma.

3.1.2 Alcances de la investigación

A) Tipo de investigación

Es de tipo **tecnológico** porque buscó dar solución a un problema encontrado en la actualidad en el ICPNA Región Centro y se utilizó tecnología existente y conocimiento teórico para resolver dicho problema.

B) Nivel de investigación

Es **descriptiva** porque detalló el proceso de cómo implementar el modelo seguridad de la información con énfasis en el factor humano y brindó los lineamientos para su mejorara en el futuro.

Es **aplicativa** porque permitió la creación de un modelo de seguridad que ayude a fortalecer el factor humano de la seguridad de la información utilizando teorías de comportamiento humano y estándares de seguridad al ser considerados en el análisis de un caso específico como es el del ICPNA Región Centro.

3.2 Diseño de la Investigación

El estudio tuvo un diseño **no experimental** porque se estableció un modelo de seguridad de la información basado en información que se obtuvo del ICPNA Región Centro y de diversas fuentes bibliográficas primarias.

3.2.1 Tipo de diseño de investigación.

La investigación tecnológica tuvo un tipo de diseño **transversal o transaccional** debido a que se deseaba conocer el estado actual de la

seguridad de la información de una empresa para poder sugerir el modelo de seguridad de la información como oportunidad de mejora.

3.3 Estudio de caso

El modelo de seguridad de la información desarrollado se basó en información recopilada del ICPNA Región Centro donde se realizó la identificación de componentes de seguridad de la información existentes y no existentes en la empresa y se contrastó dicha información con las prácticas de seguridad de la información de estándares nacionales e internacionales para la generación del modelo de seguridad de la información.

Para la fase de recolección de información se realizó la coordinación con la Presidente de Consejo Directivo y con el Gerente General del ICPNA Región Centro. A partir de un proyecto de estudio para conocer la situación actual de seguridad de la información en la institución presentado el 11 de diciembre de 2017 que fue aprobado el 26 de febrero del 2018 y formalizado el 05 de marzo del 2018, se coordinó la recopilación de información por medio de entrevistas y encuestas a personal administrativo y docente de la institución entre los días 27 de febrero y 02 de marzo del 2018. De los cuales se logró entrevistar a 37 trabajadores de ambos rubros considerando su tiempo y disposición para el apoyo del proyecto, pues era esto una condición impuesta por la dirección.

3.4 Técnicas e instrumentos de recolección de información

Con base en la naturaleza de un proyecto de investigación tecnológica, y para la elaboración del modelo de seguridad de la investigación, fue necesario contar con las técnicas e instrumentos necesarios para la recolección de información. Para esto se hizo uso fuentes primarias y secundarias, así como instrumentos de recolección de información; esta información fue necesaria para conocer cómo se está manejando el tema de la seguridad de la información en las empresas a nivel mundial y que guías, estándares y procedimientos existen en la materia, así también, conocer las iniciativas de solución ante el problema del factor humano en la seguridad de la información como punto débil; además, para conocer la realidad del ICPNA Región Centro en temas de seguridad de la información se utilizaron técnicas e instrumento de recojo de información que se describen a continuación.

3.4.1 Técnicas utilizadas en la recolección de información

3.4.1.1 Checklist

Para recopilar la información con respecto a los hábitos, cultura y necesidad de seguridad de la información en el ICPNA Región centro, se utilizó un checklist donde por medio de preguntas se especificaba el cumplimiento de los lineamientos de seguridad de la información a partir del ISO 27002, la Ley de Protección de Datos Personales (Ley 29733) y Norma Técnica Peruana NTP-ISO/IEC 27001 – 2014.

3.4.1.2 Encuesta

En base a lo anterior, se realizaron preguntas relacionadas a la seguridad de la información cuya respuesta era anotada en forma de sí y no, lo cual formaba parte del checklist, pero se realizaron también preguntas cerradas de opción múltiple donde los encuestados respondían en la base a su conocimiento, hábitos y cultura de seguridad de la información con respecto a la empresa.

3.4.1.3 Entrevista

Se utilizó la entrevista en los casos donde se requería recoger información específica y técnica sobre seguridad de la información del Sub Gerente de Tecnologías de la Información y las Comunicaciones y de la Sub Gerente de Recursos Humanos. Para este caso se utilizaron preguntas elaboradas a partir del ISO 27002, la Ley de Protección de Datos Personales (Ley 29733) y Norma Técnica Peruana NTP-ISO/IEC 27001 – 2014. La guía de entrevista se basó en preguntas cerradas y preguntas abiertas particulares a cada caso.

3.4.2 Instrumentos utilizados en la recolección de datos

El instrumento primordial utilizado es una encuesta en formato de checklist que permitió recopilar la información sobre políticas, nociones, conocimiento, costumbres y hábitos de seguridad de la información, así como de prácticas que se aplican en el ICPNA Región Centro. Este instrumento se basó en los 14 dominios, 114 controles de la ISO/IEC 27001:2013 y en los indicadores descritos en el acápite 1.4.3 y cada pregunta se orientó a conocer cada

dimensión de seguridad de la información que luego se consideraría en el modelo a diseñar.

El instrumento se dividió en 3 secciones: El primero orientado al sub Gerente de TIC con una serie de 118 preguntas cerradas y 5 preguntas abiertas a forma de guía de entrevista que estaba distribuida por temas tales como normativa y buenas prácticas de seguridad de la información, desarrollo, gestión y mantenimiento de software, data center y base de datos, ley de Protección de Datos Personales, encriptación y transmisión de datos, redes y telecomunicaciones, entre otros. La segunda sección fue dirigida a la sub gerente de Recursos Humanos, a quien se le realizó la encuesta para los trabajadores sobre temas de gestión y cultura de seguridad de la información y 13 preguntas sobre la gestión de Recursos Humanos y la seguridad de la información en particular.

Por último, la tercera sección fue orientada a personal administrativo y docente dentro de la institución; esta encuesta contenía 60 preguntas relacionadas al plan de gestión de seguridad de la información en la empresa; dirección del área de seguridad de la información; políticas, normas procedimientos e instructivos en la empresa; gestión de incidentes; capacitaciones de seguridad de la información; hábitos de protección de información; conocimiento de seguridad de la información, confidencialidad de información en la empresa y satisfacción laboral en la empresa. Todo esto como parte de conocer la cultura de seguridad de la información, donde los entrevistados podrían agregar información adicional que creyeran conveniente y que fuera relevante para el estudio. El modelo de checklist, encuesta y guía de entrevista utilizado en cada una de las áreas se encuentra en los ANEXOS 2, 3 y 4.

CAPÍTULO IV

NIVEL DE SEGURIDAD LA INFORMACIÓN EN LA EMPRESA Y MODELO DE SEGURIDAD DE LA INFORMACIÓN

4.1 Análisis del nivel de seguridad de la información en el ICPNA RC

Para la elaboración del modelo de seguridad de la información, se recopiló información del personal del ICPNA Región Centro a través de los instrumentos descritos en el capítulo anterior que consideran los indicadores de evaluación del modelo de seguridad de la información descritos en el acápite 1.4.3 y que están basados en la norma ISO/IEC 27001:2013. Dicha información recopilada proviene de 37 personas tanto del personal administrativo y docente del ICPNA Región Centro considerando su disponibilidad de tiempo y la disposición para el apoyo en el estudio. De los cuales se logró entrevistar a 35 personas de diversas edades y en diversos puestos y cargos dentro de la institución sobre conocimiento, hábitos y cultura de seguridad de la información. Del mismo modo se entrevistó de manera particular al sub gerente de Tecnologías de la Información y las Telecomunicaciones con el propósito de conocer los niveles de seguridad de la información de forma transversal al momento del recojo de información. Asimismo, se entrevistó a la sub gerente de Recursos humanos, con la finalidad de conocer como el área de Recursos Humanos se orientaba a la fecha para generar y aumentar el nivel de cultura de seguridad de la información en coordinación con la Sub gerencia de las TICs.

La información recolectada permitió conocer de primera mano la situación actual de seguridad de la información del ICPNA RC tanto por parte del área de TIC, la gerencia de Recursos Humanos y el personal en general. Esto permitió contrastar dicha situación y compararla con los indicadores de evaluación del modelo del acápite 1.4.3. Sobre todo, permitió confirmar la necesidad de fortalecimiento del factor humano de

la seguridad de la información en la empresa como un factor clave en el éxito de la gestión de seguridad de la información reflejado en el modelo. Esta información permitió diseñar un modelo acorde con la institución y acotó con información relevante para el diseño del modelo. Los resultados generales por cada categoría de la encuesta según los indicadores de evaluación del modelo de seguridad de la información y de cultura de seguridad de la información que se permitió publicar se encuentran en el ANEXO 5; la descripción consolidada de dicha información se describe a continuación:

4.1.1 Sobre el plan de gestión de seguridad de la información

De las encuestas para el área de TICs y el personal en general se encontró que no se cuenta con un plan de seguridad de la información, ni se tiene un plan en proceso de desarrollo para el corto plazo dentro de la empresa. Sin embargo, se evidenció que el 100% de los entrevistados según la encuesta al personal consideran que es necesario implementar un proyecto que pueda ayudar a proteger la información y gestionar su seguridad; y del mismo modo estarían dispuestos a apoyar activamente al mismo.

4.1.2 Sobre la dirección del área de seguridad de la información

Con respecto a este ámbito, se encontró que el 100% de los trabajadores entrevistados afirma que no existe un área de seguridad de la información establecida y reconocida en la institución. Sin embargo, aproximadamente el 17% de los entrevistados utilizando la encuesta al personal considera que el sub gerente de TI es el responsable de la seguridad de la información de manera informal debido a su cargo; esto debido a que la institución no ha designado a dicha persona como el responsable de la seguridad de la información; por lo cual, la responsabilidad de la gestión de seguridad de la información aún no se ha puesto sobre ninguna persona, lo que conlleva a una limitación en lo que se pueda hacer con respecto a la seguridad de la información en la institución.

4.1.3 Sobre la gestión de riesgos

Con respecto a la gestión de riesgos en la institución y basados en la encuesta realizada al Sub gerente de Tecnologías de la Información y Comunicaciones, se evidenció que no se tiene una gestión de riesgos implementada en la institución. Es decir, nunca se han identificado los activos de información, no

se ha realizado una identificación de vulnerabilidades de dichos activos, ni se ha realizado el estudio de riesgos dentro de una matriz que ayude a implementar controles de seguridad de la información. Por lo cual, la empresa requiere que se realice esta gestión de modo que puedan mitigar el impacto de los riesgos en la empresa y de este modo salvaguardar la información dentro de ella.

4.1.4 Sobre políticas, normas, procedimientos e instructivos en procesos de información clave de la empresa

A partir de las encuestas realizadas al Sub gerente de TIC y al personal de la institución se evidenció que no existen políticas, normas, procedimientos e instructivos claros con respecto al manejo de información que se utiliza en la institución. Sin embargo, los trabajadores de diversas áreas entrevistados afirmaron que se tienen ciertos procedimientos aplicados como el control de accesos, el bloqueo de ciertas aplicaciones y sitios web y que se les permite a los trabajadores cambiar sus contraseñas cuando lo requieren. La institución requiere que se establezcan políticas claras que guíen la seguridad de la información en la empresa.

4.1.5 Sobre la gestión de incidentes de seguridad de la información

En consideración de la información recopilada de las encuestas y checklists del estudio se encontró que no se tiene un registro de incidentes para la empresa salvo por el registro de ocurrencias que el personal de vigilancia tiene a su cargo, pero no se utiliza en la planificación ni prevención de riesgos en su área. Así mismo, se encontró que un 29% de los entrevistados según la encuesta a los trabajadores de diversas áreas, ha reportado incidentes de acceso no autorizado de personas; sin embargo, dichos reportes no han sido registrados de manera formal y se han reportado a diversas personas, en muchos casos, estos incidentes han quedado en una notificación oral. La falta de gestión de incidentes en la empresa facilita la ocurrencia de incidentes repetitivos debido a que no se realizan cambios permanentes ante incidentes registrados, tampoco se puede facilitar la toma de decisiones al respecto al no proveer a la alta gerencia con información relevante de esta gestión.

4.1.6 Sobre capacitaciones en temas de seguridad de la información

Con respecto a las capacitaciones de seguridad de la información realizadas en la institución se evidenció de la encuesta al sub gerente del área de TICs que no existe un plan de capacitaciones; lo mismo fue confirmado por todos los trabajadores entrevistados que afirmaron que no se cuentan con capacitaciones sobre seguridad de la información en el ICPNA RC. Esto genera un riesgo grave con respecto a tener el factor humano en la institución con un conocimiento escaso o nulo sobre temas necesario para la protección de la información.

Esto es preocupante debido a que el desconocimiento del personal aunado a la falta de motivación por parte de la institución para generar una cultura de seguridad de la información podría incrementar los riesgos relacionados dentro de la institución. Asimismo, la falta de políticas de seguridad de la información ha permitido que la información dentro del ICPNA RC esté en riesgo de pérdida, robo o destrucción accidental o mal intencionada. Si esto no es abordado cuanto antes, podría afectar gravemente la credibilidad y reputación de la institución ante el público y otras instituciones públicas y privadas.

4.1.7 Sobre conocimiento y hábitos de seguridad de la información

Para esta sección se consideraron diversas preguntas relacionadas con conocimiento y hábitos de seguridad de la información que se consideran necesarios al momento de tratar el factor humano de la seguridad de la información. Con respecto al conocimiento de temas de seguridad de la información en el personal en general, se evidenció que un 57% de los entrevistados de diversas áreas, no tienen ningún conocimiento sobre temas de seguridad de la información, mientras que un 34% de los mismos solo tiene un conocimiento limitado que no es ni siquiera básico. Esto se debe a que la institución no invierte en el tema, ni anima a sus trabajadores a adquirir conocimiento en seguridad de la información como se evidenció de la encuesta.

Con respecto a los hábitos de seguridad de la información, la figura 9 presenta la información encontrada con respecto al conocimiento y aplicación de hábitos de seguridad de la información donde se evidenció que un 34% de los entrevistados no tienen conocimiento, ni aplica hábitos de seguridad de la

información a nivel personal o laboral; un 57% del personal entrevistado tiene un conocimiento limitado o casi nulo del tema y sólo aplica unos cuantos hábitos que se relacionan en muchos de los casos a utilizar contraseñas. Un 6% de los tales tienen conocimiento básico de hábitos de seguridad de la información y los aplica a nivel personal y sólo 1 persona tiene conocimiento que es aplicado en lo personal, pero en lo laboral no es suficiente.

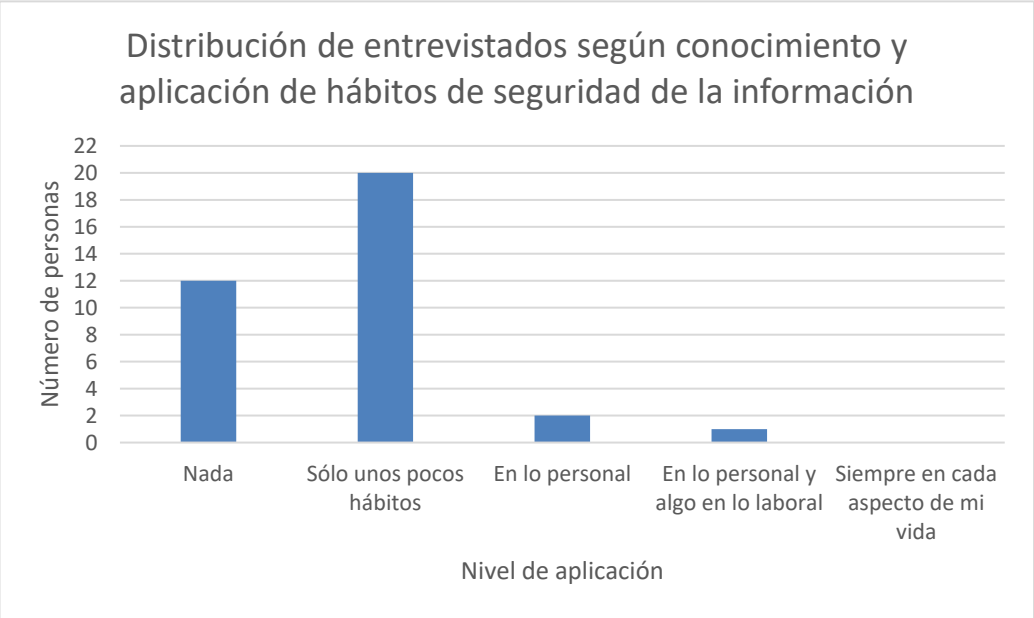

Figura 9. Distribución de entrevistados según conocimiento y aplicación de hábitos de seguridad de la información

Fuente: Elaboración propia

En esta área, también se realizaron 17 preguntas relacionadas al conocimiento y práctica de hábitos de seguridad de la información que son parte del checklist utilizado que confirmaron el nivel de conocimiento y aplicación de dichos hábitos; sin embargo, su resultado no se permitió compartir. A manera general, se evidenció de estas preguntas, que en promedio un 64% de los entrevistados del personal no practica hábitos de seguridad de la información. Esta información demostró además que se necesita un fortalecimiento urgente de los hábitos de seguridad de la información del factor humano en la institución; el cual es el propósito del modelo realizado.

4.1.8 Sobre confidencialidad de la información en la empresa

Con respecto a la confidencialidad de información en la empresa, se evidenció de las entrevistas realizadas a los trabajadores y a la sub gerente de Recursos

Humanos, que existen clausulas en los contratos sobre la confidencialidad de la información que manejan para ciertos cargos dentro de la institución: sin embargo, no se especifica que información es la que debe mantener en carácter confidencial de forma específica puesto que no hay una descripción de la información de la cual cada trabajador hace uso según lo confirmaron el 86% de los entrevistados. Además, se evidenciaron ciertas falencias técnicas con respecto al manejo de información de índole confidencial que no se publicó en este informe por ser de riesgo para la empresa.

4.1.9 Sobre la satisfacción laboral en la empresa

Uno de los factores clave de éxito que menciona la (The International Organization for Standardization, 2013) es la participación mayoritaria y activa del personal. Por lo cual, esta sección, de forma general, tuvo como propósito conocer el nivel de satisfacción los trabajadores dentro del ICPNA RC. Al procesar la información se encontró un 86% de los trabajadores de la empresa entrevistados no se encuentra satisfecho con puesto actual y los beneficios que recibe por parte de la institución. Por otro lado, sólo 4 personas se encuentran satisfechos con su actual puesto y los beneficios que recibe de la institución; de los cuales 3 de ellos se encuentran en puestos de gerencia en la institución. La figura 10 muestra la información descrita.

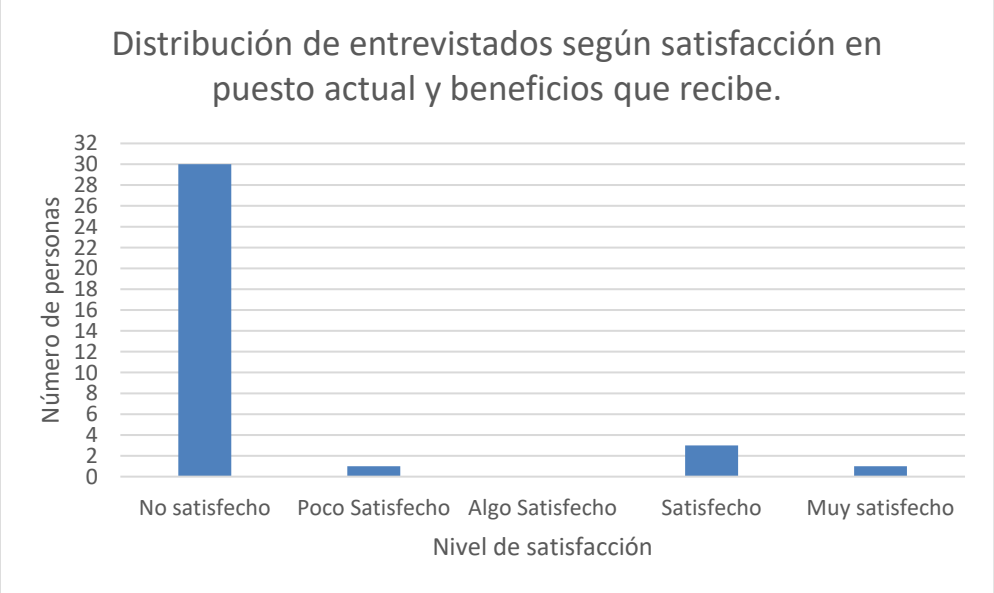

Figura 10. Distribución de entrevistados según satisfacción en puesto actual y beneficios que recibe

Fuente: Elaboración propia

Considerando que tener personal satisfecho en sus puestos de trabajo es una de las bases fundamentales para la implementación de todo tipo de gestión de seguridad de la información, la cifra de personas no satisfechas es alta; por este motivo, se requiere una evaluación de satisfacción laboral más profunda para determinar por qué el personal no se encuentra satisfecho en sus laborares; además, se necesita mejorar este indicador antes de solicitar el apoyo de todo el personal para la implementación de cualquier proyecto de gestión de seguridad de la información. Tener trabajadores insatisfechos con su labor puede generar deslealtad con la empresa y por ende ser tentados a no guardar la información la cual manejan en su lugar de trabajo; esto dificulta grandemente la generación y fortalecimiento de cultura de seguridad de la información.

En resumen, los indicadores bajo los cuales se realizaron preguntas sobre seguridad de la información en los empleados entrevistados y las respuestas obtenidas, evidencian que no existe un programa que permita gestionar la seguridad de la información y que es necesario implementarlo lo más antes posible considerando estándares y normativas nacionales e internacionales de seguridad de la información. Considerando la necesidad de gestionar la seguridad de la información, se debe realizar algún tipo de tratamiento al factor humano antes o paralelamente al implementar algún tipo de gestión de seguridad de la información en la empresa. Por lo cual, el modelo de seguridad de la información debió contener un área que fortalezca el factor humano de la seguridad de la información para el ICPNA RC.

MODELO DE SEGURIDAD DE LA INFORMACIÓN

4.2 Propósito del modelo de seguridad

El valor de la información para las empresas sin importar su tamaño va en aumento día a día debido a la competitividad creada por un incremento del número empresas en el país. Esto exige que cada organización vele por sus intereses de seguridad de modo que pueda salvaguardar la integridad, confidencialidad y disponibilidad de su información en cualquier momento del ciclo de vida de la empresa. De este punto nace la necesidad de contar con una herramienta que les permita a estas organizaciones proteger sus activos de información.

De acuerdo a la (ISO/IEC 27002, 2013), la seguridad de la información ser logrará al implementar de manera eficiente un grupo de controles que incluyen procesos, políticas, procedimientos, estructuras organizacionales y funciones de software y hardware. Por supuesto, estos controles deben estar establecidos, implementados, monitoreados, revisados y mejorados cuando se requiera, para poder asegurar que se logren los requerimientos de seguridad alineados a los objetivos empresariales.

Del mismo modo, al considerar que los activos de información están sujetos a amenazas intencionadas y deliberadas, así como de amenazas accidentales debido a que los procesos de negocio, los sistemas de información utilizados, las redes de comunicación, y los propios usuarios de los sistemas y empleados en general tienen vulnerabilidades propias a su naturaleza. Además, los cambios realizados en las empresas y sus procesos, en los sistemas que utilizan, y las propias leyes de los países donde se encuentran, como la Ley 29733 – Ley de protección de datos personales en el caso de Perú, generan también cambios que afectan la gestión de seguridad de las empresas. Por lo tanto, una gestión de seguridad de la información adecuada reducirá los riesgos generados; y lo hará de manera más efectiva y eficiente si considera el factor humano dentro de su gestión.

El modelo de información es la iniciativa de un alumno de la Universidad Continental de la Facultad de Ingeniería y de la carrera profesional de Ingeniería de Sistemas e Informática de dicha universidad. Este modelo se basa en el ISO/IEC 27002 como guía de referencia e incluye teorías sobre comportamiento humano y social para poder fortalecer el factor humano de la seguridad de la información en el ICPNA Región Centro.

Además, tiene como finalidad el ser un modelo de referencia en forma de guía práctica para poder gestionar la seguridad de la información de una empresa que tenga recursos limitados o que no pueda invertir una cantidad de dinero considerable en adquirir tecnología para poder resguardar la seguridad de la información que se considere importante y vital para dicha empresa.

4.3 Descripción y guía del modelo de seguridad de la información con un enfoque en el aspecto humano

4.3.1 Descripción

El modelo de seguridad de la información presentado toma como referencia puntos específicos del estándar ISO/IEC 27002 debido a su relevancia mundial y su trascendencia en temas de seguridad de la información. Por lo tanto, el modelo de seguridad a implementar también se centra en una gestión apropiada de riesgo de seguridad de la información; sin embargo, como valor agradado, el modelo toma también en consideración teorías de comportamiento humano y social para poder fortalecer el factor humano de la seguridad de la información y de este modo se adopta una perspectiva de la seguridad de información que considera al elemento humano dentro de las empresas como un componente necesario y factor de éxito dentro de gestión de la seguridad de la información.

El modelo propuesto se enfoca en la gestión de seguridad de la información a través de la gestión de riesgos y controles, pero lo hace a través de la óptica del factor humano debido a la participación activa del hombre en cada actividad en las empresas. Por lo tanto, considerando el factor humano como elemento clave de la seguridad de la información como se evidencia en estudios recientes como los de (Al-Mukahal y Alshare 2015), (Safa y Von Solms 2016), (Sohrabi Safa, Von Solms y Furnell, 2016), (Öğütçü, Testik y Chouseinoglou, 2016), (Safa, Solms y Futcher, 2016) entre otros, que mencionan el compartimiento del conocimiento de seguridad de la información, la creación de comunidades de seguridad de la información, la modificación de comportamiento por motivación externa, y similares como métodos efectivos para fortalecer el elemento humano de la seguridad

Además, a través de modelos elaborados, se demuestran la relación existente entre ciertas actitudes del comportamiento humano como la motivación, apego, compromiso, normas personales, colaboración entre otros, donde puede trabajarse para disminuir los riesgos de seguridad de la información; estos se basan en teorías psicológicas y sociales como la teoría de motivación, teoría de comportamiento planificado, teoría de control social con la finalidad de fortalecer el factor humano dentro de las empresas; tal como se confirma en investigaciones recientes, es el factor que mayor número de problemas causa

en la seguridad de la información según estudios de (Ponemon Institute/LLC, 2016) que incluso genera un costo millonario en las organizaciones año tras año.

Una gestión adecuada de la seguridad de la información requiere un compromiso e involucramiento de toda la empresa en su conjunto y de aquellos que formen parte de ella o que tengan contacto con ella de alguna manera, puesto que se necesita ver a la empresa como un sistema donde cada componente depende de otro y donde el pensamiento sistémico debe aplicarse para poder entender la seguridad de la información en las empresas como un ente coordinado que puede soportar los incidentes de seguridad internos y externos. Por último, se usa el ciclo de mejora continua de Deming para optimar la gestión de seguridad de la información en el modelo, y de este modo, garantizar la evolución y permanencia de la gestión de seguridad. A continuación se presenta el modelo de seguridad de la información con el enfoque en el elemento humano en el figura 11.

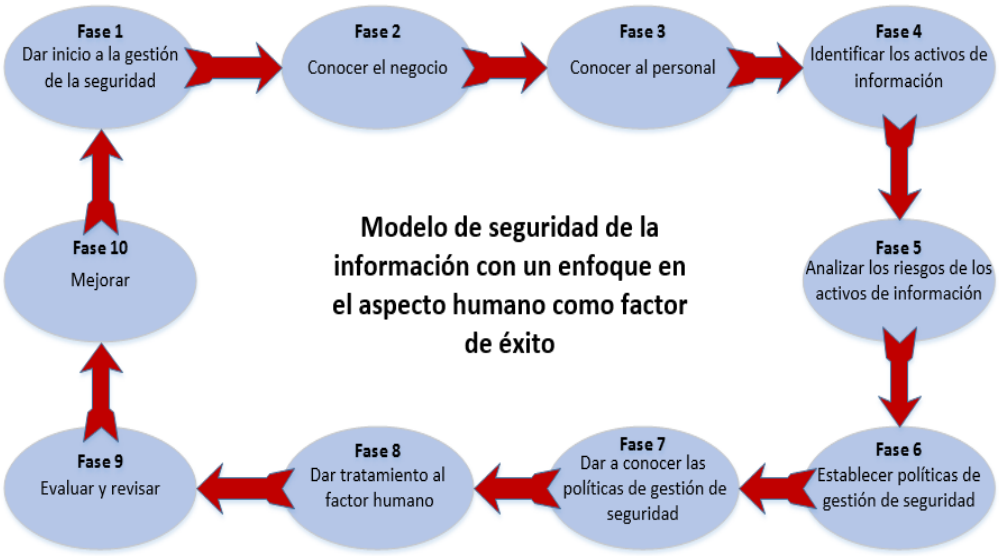

Figura 11: Modelo de seguridad de la información con un enfoque en el aspecto humano
Fuente: Elaboración propia

El modelo consta de 10 fases basadas en la parte teórica del estudio que incluyen las teorías de comportamiento humano y las normativas sobre seguridad de la información y gestión de riesgos que como iniciativa del autor consideran aspectos que buscan fortalecer el factor humano de la gestión de seguridad de la información. Cada fase es necesaria para una gestión

adecuada de la seguridad de la información con el enfoque en el factor humano. Este modelo se detalla en una guía práctica que permitirá al ICPNA RC gestionar su seguridad de la información considerando sus recursos como valiosos y limitados por la naturaleza de la empresa y al mismo tiempo que aporta una guía que puede acompañar a la empresa en los cambios que pueda experimentar en su ciclo de vida.

Una descripción sucinta de las consideraciones por cada fase se presenta a continuación:

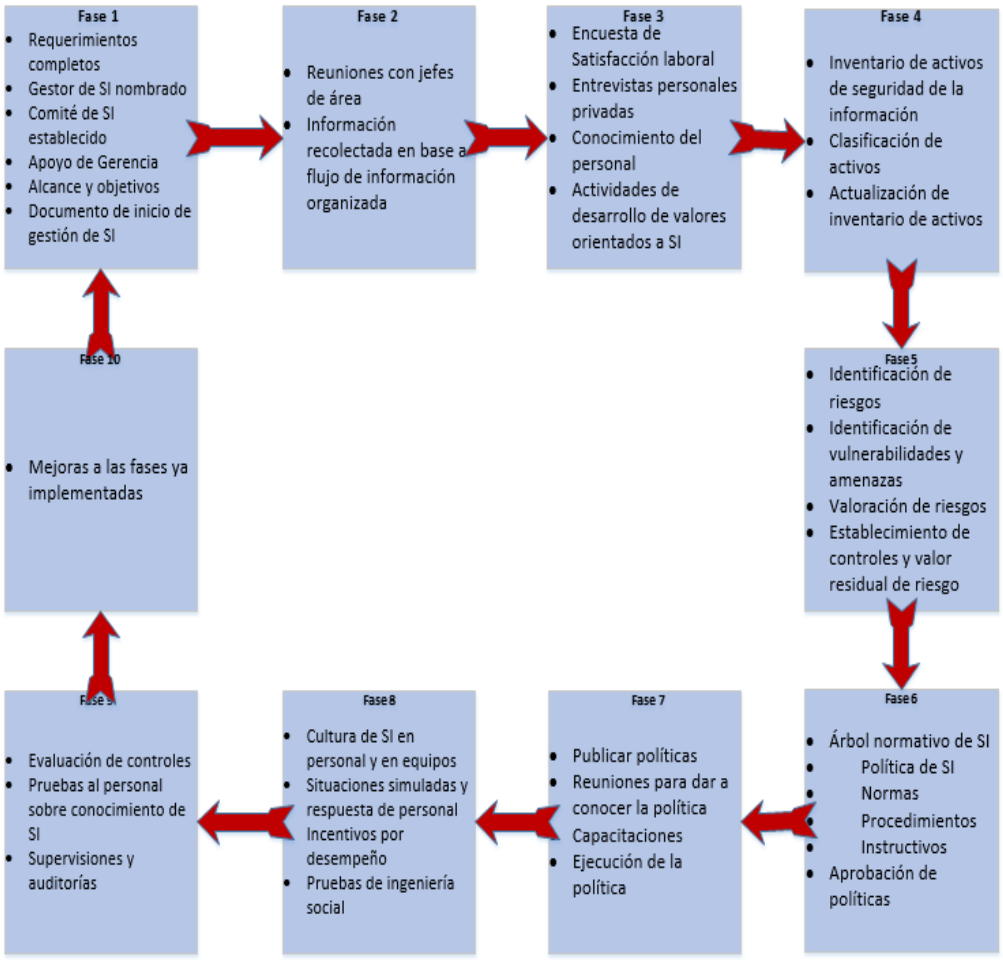

Figura 12: Consideraciones por cada fase del modelo de seguridad de la información

Fuente: Elaboración propia

4.4 Guía de Implementación del modelo de seguridad

4.4.1 Requerimientos para la implementación del modelo:

Para poder gestionar la seguridad de la información dentro de la institución, es necesario contar con los siguientes requerimientos, puesto que si no se cuenta

con uno o más de ellos, el proceso de implementación del modelo y la consiguiente gestión de la seguridad podrían fracasar por encontrarse trabas que limitan el potencial del modelo. Entre los requisitos necesarios para poder establecer el modelo de seguridad se deben considerar:

4.4.1.1 Apoyo por parte de la gerencia

Es indispensable que la alta gerencia se involucre en el gobierno y gestión de seguridad de la información debido a que este tema abarca la mayoría, por no decir todas las áreas de la empresa; por lo tanto, se necesita apoyo de la gerencia para poder coordinar cambios en los procesos de negocio que puedan carecer de seguridad en el manejo de información; del mismo modo, se requiere su apoyo para poder favorecer el cambio en las distintas áreas de la empresa, sin importar su tamaño. Por último, se necesita a la gerencia para que apruebe los documentos, políticas y planes concernientes a la seguridad de la información considerando una toma de decisiones que favorezca a la institución.

4.4.1.2 Responsable de la seguridad de la información en la empresa

El responsable puede ser una persona o un grupo de personas encargadas de la organización, planeación, evaluación y mejora del modelo de seguridad de la información dentro de la empresa. Se recomienda que el o los encargados tengan conocimientos idóneos sobre seguridad de la información y que dentro del árbol organizacional de la empresa se encuentre en un lugar estratégico para gestionar la seguridad de la información de la empresa y que brinden información que ayude a la toma de decisiones por parte de los directivos de la empresa.

4.4.1.3 Documentación acerca de la gestión de seguridad de la información

Comprenden todos los documentos necesarios para que se establezca la gestión de seguridad de la información. Entre estos documentos encontramos (los documentos serán explicados individualmente en su respectiva fase):

- Inventario de activos de información
- Matriz de riesgos y controles
- La política de seguridad de la información de la empresa.

- Indicadores de evaluación del modelo

4.4.1.4 La tecnología para proteger los activos de seguridad de la información

Es el conjunto de componentes tecnológicos como software y hardware que ayudan a la protección de los activos de información. Considerando que la tecnología, puede costar mucho dinero, se recomienda comenzar con controles de software libre y con el tiempo pensar en implementar mejores controles tecnológicos que deben ser evaluados por el responsable de la gestión de seguridad de la información.

4.4.1.5 Factor humano Capacitado

Si bien es cierto, las más populares herramientas para proteger la información son sin duda las tecnologías y por supuesto, el precio de las mejores en los mercados es de cientos de miles de dólares; sin embargo, no existe tecnología segura mientras existan personas que se encuentren detrás de las tecnologías, pues al existir error humano, los criminales informáticos utilizan a las personas para poder tener acceso a la información. Es por este motivo, que muy a pesar de contar con la tecnología apropiada, se debe contar con un personal preparado y motivado para afrontar las amenazas a la organización.

4.4.1.6 Trabajo constante con el factor humano

Este es un requerimiento clave para poder desarrollar una cultura de la seguridad de la información en los trabajadores de las empresas. Comprende las actividades relacionadas con el factor humano que ayudan a fortalecerlo ante ataques y que permite reducir los riesgos de seguridad.

4.4.2 Fases para la implementación del modelo de seguridad de la información

4.4.2.1 Fase 1: Dar inicio a la gestión de la seguridad de la información

En primer lugar, se debe comprobar si se tienen los requerimientos para implementar el modelo de seguridad de la información. Si fuera el caso de que uno o más de ellos no se tienen, se debe tratar de manejar su adquisición para poder fortalecer la seguridad de la información. Una vez que se tiene la disposición de conseguir los requerimientos mencionados,

se puede dar partida a la primera fase del modelo de seguridad; para eso son necesarios los siguientes sub pasos:

4.4.2.1.1 Establecer quien o quienes conforman la dirección y el comité de seguridad

Determinar quiénes son los encargados de implementar el modelo en la organización y quienes serán los encargados de evaluar y revisar el modelo para su mejora continua en la empresa es de vital importancia debido a que se necesita una persona o grupo responsable, con un líder a la cabeza del grupo, que pueda ayudar a mantener el primer impulso de la implementación del modelo, en cada una de las fases; además, una vez implementado el modelo, se necesita de personas que puedan revisar el funcionamiento del modelo y hacer ajustes en miras de su mejora continua.

4.4.2.1.2 Obtener el apoyo por parte de la gerencia

Es indispensable que se tenga el apoyo de los directivos de la empresa si se quiere implementar el modelo de seguridad de la información de forma efectiva; una gestión sin el apoyo de la gerencia será limitado y de cierto modo deficiente: por lo tanto, se requiere explicar de manera precisa y con términos simples y entendibles el propósito del modelo de seguridad de la información y como este puede ayudar a proteger los activos de la información. Además, es necesario obtener la confianza de los directivos en los responsables de la seguridad de la información que implementarán el modelo y que se encargarán de revisarlo.

4.4.2.1.3 Determinar el alcance y los objetivos del modelo de seguridad de la información

Una vez ganada la confianza de los directivos y establecida la persona o personas que se encargarán de gestionar la seguridad de la información, es necesario establecer el alcance y los objetivos del gobierno de Seguridad de la información. Esto implica determinar las áreas que afectará y modificará el modelo con miras a asegurar la información; también, se deben establecer objetivos claros de lo que

se quiere lograr con su implementación, alineándolos a los objetivos de la de la gerencia general; es decir, se necesita generar los objetivos de seguridad teniendo como guía los objetivos de la empresa. Cabe precisar que los objetivos son propios de cada empresa y los objetivos del modelo de seguridad dependerán, de cómo se hayan determinado y hacia qué rumbo apuntan los objetivos empresariales; en este caso los del ICPNA RC.

4.4.2.1.4 Asignar las facultades a los encargados de la seguridad

Una vez establecidos el alcance, los objetivos, los encargados y se ha obtenido el apoyo de la gerencia, se debe redactar un documento que dé inicio al área de seguridad de la información en la empresa como tal, en el caso que no existiera; si ya existe, el documento ratifica el área y especifica las funciones y características del área. El documento debe contener la siguiente información:

- El acuerdo de la gerencia, es el acuerdo final como consta en el acta de reunión de los directivos o en su defecto, la autorización del responsable de la empresa sobre el responsable o responsables de la seguridad de la información. En ambos casos dando su confianza y respaldo en la implementación del modelo
- El alcance del modelo de seguridad
- Los objetivos del modelo de seguridad
- Identificar los Stakeholders (Partes interesadas), se debe especificar quienes (que áreas y los encargados) serán los directamente afectados con la gestión de seguridad.
- La descripción de la fases del modelo de seguridad que se implementará
- Las firmas que dan validez al documento incluyendo la del jefe encargado de la implementación del modelo.

Por último, el documento debe ser publicado y compartido en todas las áreas de la empresa. Además, se debe tener una reunión con los gerentes o jefes de departamento para dar a conocer las ventajas y la necesidad de implementar el modelo de seguridad. Además, se recomienda una reunión con todo el personal de la empresa y dar a conocer el proyecto de implementación del modelo con sus ventajas

y beneficios, pero enfatizando la necesidad de colaboración de todos ellos para hacer que el modelo sea efectivo.

Se recomienda en cada caso incorporar al gestor y a su equipo (si fuera el caso) en el organigrama de la empresa bajo la supervisión del directorio o de gerencia general y como un órgano independiente de toda otra área. Esto es importante porque brindará al gestor la capacidad de trabajar en aras de la protección de la información de la empresa.

4.4.2.2 Fase 2: Conocer el negocio

Para esta fase, el documento de inicio del área de seguridad y del proyecto de seguridad de la información ya existe y por lo tanto, el gestor de la seguridad de la información ya tiene la capacidad de planear actividades, organizar reuniones, establecer políticas, entre otros con el objetivo de implementar el modelo. Ahora se debe conocer el negocio. Si el gestor es parte del negocio y proviene de algún área en particular, se recomienda que integre el conocimiento de todas las áreas considerando la empresa como un todo, además que cada área o departamento depende de otros y que su interacción conectada con las otras áreas es vital. Para esto debe solicitar reuniones con los responsables de cada área para entender cómo es que funciona el área en cuestión tal y como esta. Esta función del gestor de la seguridad es importante debido a que al interactuar con los responsables o gerentes de otras áreas, podrá identificar como es que funciona el negocio con miras a proteger los activos existentes en cada uno de ellos. El Gestor de la seguridad necesita realizar lo siguiente:

- Establecer reuniones con todos y cada uno de los responsables o gerentes de las áreas.

  Se pueden abordar temas relacionados a:
  - Explicación del propósito de su visita (Se recomienda grabar la conversación con la autorización del entrevistado explicando que esa información es necesaria para conocer el negocio como tal)
  - Área de la que se encarga
  - Número de personas que dependen de su cargo y sus cargos respectivos
  - Propósito del área

    - Actividades que realiza su área
    - Con que otras áreas interactúa
    - Solicitar información específica del área de forma impresa o como documento electrónico, si existe.
    - Evaluación del personal a su cargo. ¿Cómo se hace?
    - Qué tipo de información maneja en su área
    - Proyectos del área implementados o por implementar
    - Explicación del proyecto de implementación del modelo
    - Obtención de apoyo en la implementación del modelo (Si fuera el caso de una respuesta negativa, se recomienda ser empático y tratar hacer valer el documento de gerencia)
- Solicitar una visita al área en cuestión para ver cómo se desarrollan las actividades de los empleados. Se recomienda utilizar una cámara de video, con autorización del gerente del área, para ver el proceso de negocio y donde se realiza.
- Ser amable en todo momento con los trabajadores y mostrar empatía al visitar sus lugares de trabajo; es vital obtener la confianza del personal en este momento.

  Una vez recolectada la información, es necesario realizar lo siguiente:
- Utilizar el organigrama de la empresa, si se tuviera, o realizar un mapa organizativo de las áreas entrevistadas identificando los nodos o puntos principales del negocio.
- Identificar los lugares donde el uso de información se hace más relevante.
- Realizar una descripción del área visitada considerando los puntos más resaltantes de área tal y como está, evitando todo juicio que pueda comprometer la descripción precisa del área en cuestión.

Esta información es el segundo paso del modelo de seguridad de la información, y es relevante debido a que con ella se podrá conocer en una primera instancia a los directamente involucrados con la información de la empresa, así como de su entorno de trabajo y su relación con sus jefes. Además, se tendrá información sobre los trabajadores para poder realizar la fase 3 del modelo.

4.4.2.3 Fase 3: Conocer al personal

Esta fase es crucial para el modelo de seguridad de la información con énfasis en el factor humano debido a que el conocimiento del personal llevará determinar las actividades que ayudarán a crear una cultura de seguridad de la información y nos brindará una idea de las áreas a fortalecer en temas de comportamiento humano y de seguridad de la información. Por lo tanto, el modelo, enfoca su fortaleza en el factor humano como una cuestión que complementa la tecnología puesto que por sí sola la tecnología es insuficiente para proteger los activos de información. (Sohrabi Safa, Von Solms y Furnell 2016). De este modo, un entendimiento de los factores de comportamiento y satisfacción de las personas puede ayudarnos a tener una mejor planificación de cómo hacer crecer la cultura de seguridad de la información.

Para poder tener una identificación y conocimiento del personal se sugieren las siguientes técnicas:

- Utilizar una encuesta de satisfacción laboral es un buen comienzo
  Si se desea conocer la situación de los trabajadores de forma efectiva y saber en qué nivel se encuentra la satisfacción personal y colectiva de la empresa, se puede realizar o utilizar una encuesta de satisfacción laboral que contemple las necesidades básicas o fisiológicas, de seguridad, sociales, de estima y autorrealización de la pirámide de Maslow (Clonninger, 2002 p. 462). En el caso se desee elaborar una encuesta, los siguientes temas pueden ser utilizados:
  - Satisfecho con la remuneración
  - Satisfecho con su lugar de trabajo
  - Satisfecho con sus funciones y responsabilidades
  - Satisfecho con los materiales que tiene para realizar su labor
  - Satisfecho con los contratos y estabilidad laboral
  - Satisfecho con los empleados de la empresa que dependen de uno.
  - Satisfecho con los supervisores y superiores
  - Satisfecho con los compañeros de trabajo
  - Satisfecho con el trato que recibe en su trabajo
  - Satisfecho con capacitaciones brindadas por la empresa
  - Satisfecho con las posibilidades de crecimiento personal y profesional

- Satisfecho con las políticas de ascenso
- Preguntas abiertas sobre información relacionada a la empresa
- Otros que considere relevantes en la empresa y que haya notado.

- Tener entrevistas personales con los trabajadores de diversas áreas de forma anónima. Esto puede brindarle una perspectiva al gestor o a su equipo de cómo es en realidad el funcionamiento de la empresa; la privacidad de la entrevista puede darle información que no se pudo identificar en la fase de conocer el negocio. Estas entrevistas pueden ser sustituidas por preguntas abiertas en el cuestionario de satisfacción del personal.
- Si se considera un examen psicológico antes de la contrata del personal, se puede considerar recopilar información directa de esta fuente para poder identificar características del comportamiento de los empleados. Si no se ha considerado un examen de psicológico para la contrata, pero se cuenta con el área de psicología dentro de la empresa, se puede sugerir incluir preguntas brindadas por el psicólogo que puedan ser incluidas en el cuestionario de satisfacción laboral como un aspecto aparte pero necesario. Esta información, dará una versión más reciente de la información sobre el estado psicológico y de comportamiento de las personas. Se recomienda, también, incluir estas preguntas si se desconfía de la información sobre los exámenes psicológicos antes de la contrata o si se desea información más actual. Si fuera el caso que no se cuenta con un área psicológica en la empresa, se puede contratar a un profesional que haga las labores dentro de la empresa por un tiempo determinado. Por último, si no se desea contratar a un psicólogo para todo el estudio, se le puede contratar para realizar las preguntas dentro del cuestionario y para consolidar los resultados de los mismos.
- Se debe consolidar los resultados de las encuestas y/o entrevistas con el personal para poder establecer un documento guía que permita desarrollar capacitaciones, charlas, talleres y entrenamiento que ayuden a formar valores y características del comportamiento adecuados a la cultura de seguridad de la información.
- Se debe coordinar con el área de recursos humanos, el desarrollo de actividades orientadas a generar valores como honestidad,

responsabilidad, voluntad, prudencia, entre otros necesarios para la implementación del modelo de seguridad de la información con el enfoque en el factor humano. El tratamiento del personal comienza desde este punto, puesto que cuando se implementen las políticas de gestión de la seguridad descritas más adelante, se necesitará de todo el tratamiento conductual posible para lograr una asimilación de las mismas.

- En coordinación con el área de recursos humanos, se debe dialogar con la gerencia sobre los temas que presentan insatisfacción laboral en el personal. Mostrando los resultados obtenidos en la encuesta de satisfacción y/o entrevistas, se debe enfatizar la importancia de realizar cambios que motiven al personal y los preparen para la gestión de la seguridad de la información de forma más identificada con la empresa. También se recomienda utilizar técnicas de fidelización del personal, y salario emocional como técnicas donde puede trabajar el área de recursos humanos con la participación de un psicólogo. Si bien es cierto, es decisión de la empresa, esto, aumentará la probabilidad de éxito del modelo considerando los modelos conductuales considerados.
- Los pasos mencionados anteriormente, no sólo ayudarán al modelo de seguridad a implementar y a la gestión de la seguridad de la información, sino que también ayudarán a otras áreas de la empresa y se tendrá personal con un mejor estado anímico para desarrollar sus actividades; por lo tanto, esto significará beneficios para la empresa.

Ahora bien, se necesita un presupuesto para las capacitaciones y los cambios a realizar en la empresa. En este punto, las capacitaciones deben ser agendadas en los primeros costos de implementación del modelo; sin embargo, el costo de conocer al personal y empezar a trabajar en él, redituará en beneficios para la empresa y los trabajadores, aun si no se implementara el modelo. Finalmente, conociendo el negocio y el factor humano, se puede realizar el siguiente paso e identificar los activos de información.

4.4.2.4 Fase 4: Identificar los activos de información

Para comenzar a tratar el área de políticas y tecnológica de la seguridad, es necesario comenzar por lo que se desea proteger, los activos de

información. Para lo cual, se debe conocer que son los activos de información y como se clasifican.

4.4.2.4.1 Definición

Los activos de información, según (ISO27000.es, 2016) se definen como: “(Inglés: Asset). En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.” Los activos son importantes para la seguridad de la información debido a que no se podría dar protección a los que no se conoce. Es decir, no se puede asegurar la confidencialidad, disponibilidad e integridad de la información, aun así sea clave para la empresa si no se conoce cual es esta información.

4.4.2.4.2 Clasificación

El estándar (ISO/IEC 27002, 2013) indica que los activos de información tienen que ser identificados en su totalidad de forma precisa y clara para poder construir un inventario de activos de la información que debe ser actualizado periódicamente y que contenga los más importantes activos de la información. Estos activos pueden clasificarse en:

- **Información:** se incluyen bases de datos, archivos, licencias, documentación, material de formación, manuales de usuarios, procedimientos, planes de continuidad de negocio, contratos, etc.
- **Software:** Sistemas operativos, software de aplicaciones, sistemas de información, interfaces, programas y herramientas de desarrollo, etc.
- **Físicos:** Servidores, PCs, laptops, dispositivos móviles, equipos de comunicación, periféricos, equipos de protección eléctrica, etc.
- **Servicios:** servicios de comunicación, servicios de internet, servicios generales, etc.
- **El personal:** hace referencia a personal que posee información.
- **Intangibles:** reputación, imagen de la organización, etc.

Para poder identificar y tener un inventario de activos relacionados con la información que se desea proteger, se puede comenzar

utilizando el inventario de existencias de equipos informáticos de la empresa, si es que se tiene, o si no se cuenta con uno, se puede empezar con el inventario de activos desde cero. Si el inventario físico patrimonial de tecnologías de la información existe, este nos dirá que buscar y donde encontrarlo; sin embargo, sea que exista uno o no, se debe considerar una visita a todas las áreas de la empresa donde se encuentren activos que se desean proteger.

Se recomienda utilizar el formato provisto como anexo, o cualquier otro formato que ayude a la identificación, clasificación y ordenamiento de los activos. Para poder conocer los activos más importantes, se recomienda realizar un filtrado de la información.

El formato que se provee tiene los siguientes campos de consideración:

- **Código de Activo:** Es el código que se le asigna al activo para el inventario. Este código depende de la empresa.
- **Nombre del Activo:** Comprende el nombre del activo que se identifica.
- **Descripción del activo:** Se escribe la descripción detallada del activo con información como propósito, marca, número de serie, tipo, información técnica, color, estado del activo, forma de almacenamiento, etc. Es decir, se incluye información que sirva para poder identificar para que se usa el activo y sus características para poder identificarlo. Se recomienda obtener esta información del inventario de activos físicos de la empresa del área de patrimonio si es que se tuviera en el caso de activos físicos.
- **Área de la empresa:** Describe el área de la empresa donde se encuentra el activo. Se recomienda actualizar este campo si se realiza un cambio en la localización del activo.
- **¿Dónde se almacena?:** Se especifica el lugar donde se almacena esta información. Se recomienda ser especifico; lugar digital y físico dependiendo del caso.
- **Naturaleza del activo:** Describe si el activo es tangible o intangible. Esto determina su almacenamiento. En el formato propuesto se puede seleccionar una de las opciones.

- **Clasificación:** La clasificación de los activos de información es vital para poder determinar que activos deben ser protegidos con mayor esfuerzo que otros; además, se utiliza para determinar los niveles de acceso a estos. En el formato propuesto se puede seleccionar una de las tres opciones. Entre la clasificación que se le da al modelo se incluye:
    - **Criticidad:** Describe que tan crítico es este activo para la empresa en términos de importancia y necesidad. El activo se designa como crítico si su falla o falta ocasiona la interrupción para el proceso.
    - **Frecuencia de uso:** Describe con cuanta frecuencia se utiliza este activo; se debe pensar en términos de número de días por mes.
    - **Tecnología:** Esta clasificación describe el nivel de innovación tecnológica que tiene el activo, esto se relaciona también a su valor en el mercado y grado de obsolescencia.
- **Clasificación final de activo:** En este campo se determina la importancia final del activo para la empresa en cuanto a si se debería poner especial atención en su protección. En el formato propuesto, este campo se obtiene al completar el nivel de clasificación entre Alta, Media y Baja criticidad, frecuencia de uso y tecnología. Además, el formato muestra de color rojo aquellos activos que tengan alta importancia para la empresa o el área en cuestión; muestra de color ámbar, aquellos activos que tengan importancia media y de color verde aquellos activos que no requieren protección adicional.
- **Custodio del activo:** Este campo hace referencia a la persona que se encarga de custodiar este activo. Conocer esta información determinará luego la asignación de funciones y responsabilidades.

El inventario de activos, no puede ser un documento estático, puesto que siempre se realizan cambios en él; por este motivo, se deben actualizar el inventario cuando se registre algún cambio. El conocer donde se encuentran los activos y quien los custodia es necesario para poder mejorar la gestión de seguridad en los siguientes ciclos del modelo de seguridad. Una vez obtenido el inventario de activos relacionados a la

información de la empresa, se puede comenzar con el análisis de riesgos de estos activos.

4.4.2.5 Fase 5: Analizar los riesgos de los activos de información

Según (Amutio Gómez, 2012) de la metodología MAGERIT para análisis de riesgos, se define riesgo como la "estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización;" en palabras sencillas, se define el riesgo como la probabilidad de que una amenaza se aproveche de una vulnerabilidad para causar daño en los activos de información. Además nos indica (Amutio Gómez, 2012) que "El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema." En esta etapa, se deben seleccionar los activos de información que tengan una clasificación alta y media y que la alta gerencia considere urgente de tratar. De ahí el punto de partida para el análisis de riesgos.

En el análisis de riesgos se deben considerar las amenazas que pueden afectar al activo y vulnerabilidades que el activo presenta; asimismo, se debe considerar la probabilidad de ocurrencia de la amenaza y el impacto que esta tendría sobre el activo de información. Con esta información se puede estimar un valor del riesgo que nos va a ayudar a poder gestionar los riesgos que se deben mitigar con mayor urgencia dentro de la empresa. Ahora bien, la identificación de los riesgos y su valoración no son suficientes; se necesita una gestión efectiva de los mismos con respecto a que controles se debe implementar para poder reducir el riesgo. Además del control, se necesita estimar en qué manera el control implementado reduce el valor de riesgo al final, obteniendo un valor del riesgo residual que nos mostrará de qué manera estamos gestionando los riesgos con la implementación de los controles.

Con respecto a la identificación de riesgos, se necesita conocer el negocio y cuáles son las amenazas que podrían atentar contra la integridad, disponibilidad y confidencialidad de los activos. Para esto se necesita hacer un trabajo conjunto con el responsable del área, y si fuera el caso,

con algún experto en un proceso específico para poder conocer sobre las amenazas y vulnerabilidades del activo. Si bien es cierto, aunque el proceso sea algo tedioso, los beneficios del apoyo del personal directamente involucrado generaran una matriz de riesgos más robusta.

Para la elaboración de la matriz de riesgos se puede utilizar cualquier formato existente en el mercado; sin embargo, este modelo de seguridad de la información ofrece un formato de matriz de riesgos que contempla lo mencionado anteriormente y además, una lista de posibles amenazas que se pueden considerar en la elaboración de la matriz. Del mismo modo, se incluye el cuadro descriptivo de los valores a considerar en cada uno de los casos para la valoración de los riesgos. Entre los riesgos que se pueden presentar en las empresas se encuentran (Presidencia de la República de Colombia, 2013):

- **Riesgo Estratégico:** Estos riesgos se relacionados con la misión de la empresa y con el cumplimiento de objetivos estratégicos propuestos por la gerencia, y las políticas institucionales.
- **Riesgos de Imagen:** Estos riesgos se relacionan con la confianza y percepción de otras personas hacia la empresa.
- **Riesgos Operativos:** Estos riesgos que provienen del funcionamiento y la operatividad de los sistemas de información dentro de la empresa, también de la definición de procesos, de la estructura de la entidad, etc.
- **Riesgos Financieros:** Se relacionan con el manejo de recursos económicos de la empresa.
- **Riesgos de Cumplimiento:** Estos riesgos se asocian con el cumplimiento de requisitos legales, contractuales, de ética pública, compromiso ante la comunidad, etc.
- **Riesgos de Tecnología:** Estos se relacionan con la capacidad tecnológica de la empresa para satisfacer sus necesidades actuales y futuras en términos tecnológicos.
- **Riesgos de corrupción:** Se entiende por riesgo de corrupción a la posibilidad de que, por acción u omisión, mediante el uso indebido de poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del estado, para la obtención de un beneficio particular.

Para el modelo de seguridad de la información planteado se sugiere utilizar la matriz de riesgos que se adjunta como anexo y esta representa los siguientes campos:

- **Código del Activo:** Es el código que se le asigna al activo para el inventario. Este código depende de la empresa. Se recomienda copiar el código del inventario de activos.
- **Nombre del Activo:** Comprende el nombre del activo que se identifica. Se recomienda copiar el nombre del inventario de activos.
- **Vulnerabilidad:** Hace referencia a la debilidad que presenta el activo. Esta debilidad puede presentarse en su naturaleza, en su estructura, en su programación (sistemas informáticos), en su transmisión (redes), en su material, en su funcionamiento, en su utilización, etc. Es necesario hacer las correcciones sobre las vulnerabilidades, pero se recomienda que estas sean realizadas como parte de la gestión de los riesgos identificados y de controles establecidos para no causar confusión, salvo que estas vulnerabilidades representen un grave asunto para la empresa; en este caso, la acción es indispensable. Para poder definir correctamente la vulnerabilidad, se recomienda conversar con alguien entendido en el activo, de preferencia se sugiere contactar a la misma persona que se consideró para el inventario de activos.
- **Amenaza:** Se denomina así a la "Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización" (Amutio Gómez, 2012). Para el modelo, se debe considerar que las amenazas siempre corresponden a una vulnerabilidad y se deben considerar juntas. Por lo tanto, al hablar de vulnerabilidades, debemos también pensar en las amenazas. Existe la posibilidad que varias amenazas tomen ventaja de una vulnerabilidad, por lo tanto, estas amenazas deben también se consideradas en cada vulnerabilidad dentro de la matriz.
- **Código de riesgo:** Al igual que con los activos de la información, la empresa puede designar un código para poder identificar sus riesgos. Se pueden tener varios riesgos por cada amenaza identificada, incluso existe la posibilidad de que existan varios riesgos para cada amenaza identificada, y por lo tanto, deben considerarse estos riesgos dentro de la matriz

- **Riesgo (Detallar):** En esta sección se establece un nombre para el riesgo; se recomienda ser explícito con respecto al riesgo, el nombre debe ser detallado y no debe ser ambiguo.
- **¿Qué origina el riesgo?:** Esta sección describe al responsable de la causa del riesgo; esta causa puede ser una persona (interna o externa), un proceso, un sistema, etc. Se debe tener claro quién es el que desencadena el riesgo; se recomienda dialogar con los conocedores del activo sobre este asunto también.
- **Consecuencia del riesgo:** En esta área se debe plantear cual sería la consecuencia de no hacer nada al respecto del riesgo. Esta sección nos ayudará a pensar en cuán grave puede ser el riesgo y nos ayudará en la valoración del riesgo. Para poder establecer claramente la consecuencia del riesgo, se recomienda dialogar con los directamente involucrados con el activo.
- **Probabilidad de ocurrencia:** El valor de esta sección se determina por los valores de probabilidad establecidos en el cuadro de valoración de riesgos. Esta escala ha sido determinada como parte del estudio y considerando metodologías como MAGERIT entre otros ejemplos de gestión de riesgos de otros modelos de gestión de seguridad de la información. Esta escala tiene valores entre 1 y 5; donde 1 representa la probabilidad de ocurrencia más baja y 5 presenta la probabilidad de ocurrencia más alta tal como lo muestra el siguiente cuadro:

Tabla 2. Probabilidad de Ocurrencia

PROBABILIDAD DE OCURRENCIA	MUY ALTA	**5**
	ALTA	**4**
	MEDIA	**3**
	BAJA	**2**
	MUY BAJA	**1**

- **Impacto sobre el activo:** El impacto del riesgo representa la gravedad que tendría el riesgo sobre el activo si se materializa. En este caso la escala que se utiliza en el formato del modelo tiene

valores entre 1 y 5; donde 1 representa el impacto más bajo y 5 presenta el impacto más alto tal como lo muestra el siguiente cuadro:

Tabla 3. Impacto del riesgo

IMPACTO DEL RIESGO				
MUY BAJO **1**	BAJO **2**	MEDIO **3**	ALTO **4**	MUY ALTO **5**

- **Valor del riesgo:** El producto de la probabilidad y el nivel de impacto nos da como resultado el valor del riesgo. Este valor se categoriza según el cuadro de valoración de riesgos; donde se debe considerar que riesgos que tengan valores de riesgo marginal y riesgo apreciable; es decir, de color verde y amarillo, son riesgos que debemos tener en cuenta, pero se debería considerar si se implanta un control o no; por lo tanto, dependerá de factores económicos y de la aprobación al respecto de la gerencia para implementar. Sin embargo, en los riesgos que tengan valores de riesgo importante y riesgo muy grave; es decir, de colores anaranjados y rojo, necesitan de atención prioritaria de forma obligatoria y urgente respectivamente. Se recomienda filtrar los activos y riesgos en función de los valores de riesgo del formato para luego poner controles a los riesgos importantes y muy graves; esto debido a la gravedad de los riesgos. La valoración de los riesgos se da por los colores y valores del siguiente cuadro:

Tabla 4. Cuadro de Valoración de Riesgos

Cuadro de valoración de riesgos			IMPACTO DEL RIESGO				
			MUY BAJO 1	BAJO 2	MEDIO 3	ALTO 4	MUY ALTO 5
PROBABILIDAD DE OCURRENCIA	MUY ALTA	5	5	10	15	20	25
	ALTA	4	4	8	12	16	20
	MEDIA	3	3	6	9	12	15
	BAJA	2	2	4	6	8	12
	MUY BAJA	1	1	2	3	4	5

	Riesgo muy grave. Requiere medidas preventivas urgentes. No se debe iniciar el proyecto sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo.
	Riesgo importante. Medidas preventivas obligatorias. Se deben controlar fuertemente llas variables de riesgo durante el proyecto.
	Riesgo apreciable. Estudiar económicamente ai es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas.
	Riesgo marginal.Se vigilará aunque no requiere medidas preventivas de partida.

- **Estrategias de respuesta al riesgo:** En esta sección se debe elegir la respuesta que se puede tomar al afrontar el riesgo. Esto dependerá de los controles que se identifiquen para tratar con el riesgo y de la factibilidad económica y tecnología de la empresa. En algunos casos se preferirá evitar el riesgo, tal vez eliminarlo o quizá se deba transferir el riesgo a otra empresa o compañía especializada o probablemente se prefiera mitigar el riesgo a un mínimo posible aceptable o simplemente aceptarlo para no implementar algún control adicional; aunque siempre debe ser monitoreado. Esta sección ayuda a la toma de decisiones sobre los controles y viceversa.
- **Controles de riesgo propuestos:** En este apartado se deben considerar los diferentes controles específicos para los riesgos. Entiéndase como control las acciones que se deben tomar para confrontar el riesgo. Se recomienda asignar controles a aquellos riesgos importantes y muy graves; sin embargo, dependerá de la empresa también implementar o al menos diseñar controles para los riesgos apreciables y marginales. En el formato, se recomienda poner todos los posibles controles que se puedan identificar para la gestión de los riesgos según la estrategia que se tome.

- **Estimado de efectividad de los controles:** En esta sección se debe establecer un valor que pueda representar de forma numérica la efectividad de los controles establecidos; este valor deberá tener valores entre 1 y como máximo, el valor del riesgo que resultó como producto de la probabilidad y del impacto del riesgo. Este valor es un aproximado de cuán efectivo serán los controles en conjunto para tratar con el riesgo.
- **Riesgo residual:** El riesgo residual se calcula al dividir el valor del riesgo y el estimado de efectividad de los controles. Este valor nos dará una idea a priori (al inicio) y a posteriori (luego del establecimiento del modelo) de la gestión de los riesgos.

Se recomienda filtrar los riesgos muy graves e importantes para poder dar prioridad a la ejecución del control. Teniendo en claro cuáles son los activos y los riesgos que estos presentan, se debe proceder a la política de gestión de seguridad de la información.

4.4.2.6 Fase 6: Establecer políticas de seguridad de la información:

El documento guía por excelencia de lo que se debe hacer en la gestión de seguridad de la información es la política de seguridad de la información. Sin embargo, no sólo se debe considerar la política, sino que también se necesitan documentos específicos para que la gestión de seguridad de la información se cumpla a cabalidad; entre estos documentos se debe tener (ISO/IEC 27002, 2013) los procedimientos necesarios para la gestión; las instrucciones, checklists y formularios y por último los registros que sirven como evidencia del cumplimiento de los otros tres tipos de documentos . La suma de estos documentos da lugar al árbol normativo de la seguridad de la información. Ahora se describirá cada tipo de documento y se mostrará cómo establecer cada uno de ellos.

4.4.2.6.1 Política de seguridad de la información

El primer documento y el más general sobre las obligaciones y responsabilidades de los custodios de los activos; así como de los encargados de la gestión de riesgos se encuentra normado en este documento; del mismo modo se norma el uso de la información según el rubro de negocio y según los activos identificados. Además, se

brindan las pautas de cómo deben proceder los usuarios con la información que manejen; por lo tanto, se recomienda utilizar un lenguaje comprensible debido a que se necesita que los usuarios y custodios de los activos comprendan cada una de las políticas; por este motivo, se debe evitar tecnicismos que compliquen la comprensión, salvo por cuestiones técnicas que si requieran esta especificación. En la política de seguridad de la información, se establecen obligaciones derivadas de los controles de riesgos identificados que ayuden a salvaguardar la información. A continuación se muestra el contenido probable considerando el (ISO/IEC 27002, 2013) y el trabajo de (Achiary, 2005) pero con algunas consideraciones propias del autor; por supuesto, este formato dependerá del alcance de la gestión y de las necesidades de la misma. El contenido probable de una política de seguridad de la información tiene los siguientes elementos:

- **Introducción:** Esta sección muestra de forma global el contenido de la política de la seguridad de la información. Se debe plantear la visión global de la misma y lo que se desea lograr con la política de seguridad de la información.
- **Aspectos generales:** En esta sección se presentan aspectos relativos a la gestión, dirección, y organización del área de seguridad y de la política de seguridad. Como parte de esta sección se tiene:
    - **Alcance:** El alcance de la política de seguridad de la información debe concordar con el documento de la Fase 1; es decir, el alcance debe mantenerse, salvo que luego de la identificación de los activos y el inicio de la gestión de riesgos, se necesite dar un ajuste a esta sección; si este fuera el caso, se deberá actualizar el primer documento y utilizar el nuevo alcance en esta sección.
    - **Declaración de autoridad:** Se designa sobre quien o quienes recae la responsabilidad de la gestión de seguridad de la información, para este modelo se le denomina Gestor de la seguridad. Además, se mencionan los cargos del equipo que acompañaran al gestor, estos cargos dependerán de lo que decida la alta dirección.

- **Objetivos de la política:** Se deben plantear los objetivos que se desea para la gestión de seguridad. Se recomienda utilizar los mismos objetivos de la fase 1, salvo que luego de la identificación de los activos y del manejo de riesgos, se necesite dar un ajuste a esta sección; si este fuera el caso, se deberá actualizar el primer documento y utilizar los nuevos objetivos en esta sección.
- **Términos y condiciones de uso:** Se debe establecer una cláusula que determine la privacidad y utilización del documento dentro del ámbito de la empresa.
- **Definición de términos:** Esta sección contiene los términos clave que se encontrarán en la política de seguridad de la información. Estos términos deben ser definidos utilizando palabras comprensibles, y de fácil acceso para el personal. Además, por razones de derechos de propiedad intelectual, se recomienda citar toda fuente de donde se obtengan los términos, si estos no contienen definiciones propias.

- **Organización de la seguridad:** En esta sección se determina cómo se organiza la gestión de la seguridad de la empresa y quienes son los responsables de dicha seguridad. En este punto se pueden considerar:
  - **Comité de la seguridad de la información:** Se deben especificar los nombres de las personas (no necesariamente del área de seguridad de la información) que colaboran con la seguridad de la información; puede estar compuesto por gerentes, directivos u otras personas de influencia que colaboraren en la seguridad de la información.
  - **Asignación de responsabilidades en la gestión de seguridad de la información:** En esta sección se deben incluir los nombres de los responsables de la seguridad en los procesos de seguridad.

Tabla 5. Cuadro de Asignación de Responsabilidades

Fuente: (Achiary, 2005)

Proceso	Responsable
Seguridad del Personal	.....
Seguridad Física y Ambiental	.....
Seguridad en las Comunicaciones y las Operaciones	.....
Control de Accesos	.....
Seguridad en el Desarrollo y Mantenimiento de Sistemas	.....
Planificación de la Continuidad Operativa	.....
.....	.....

Del mismo modo se deben especificar los propietarios de información por cada área de la empresa; ellos serán los responsables de seguridad de sus áreas.

- **Autorización para instalaciones de procesamiento de información:** En esta sección se debe indicar quien es el que autoriza la instalación de nuevo software y se describe el motivo por el cual se hace esto. Se recomienda que sean autorizadas por los responsables de seguridad de sus áreas en coordinación con el gestor de la seguridad de la empresa.
- **Asesoramiento en temas de seguridad de la información:** Aquí se menciona quien será la persona o personas encargadas de asesorar al personal en cuestiones de seguridad de la información. Se recomienda que sea el gestor de seguridad por ser el más entendido en la materia o personal que este designe.
- **Auditoria de la seguridad de la información:** se debe mencionar la posibilidad de auditar los procesos de seguridad de la información en búsqueda de riesgos y mencionar quien hará estas auditorías. La auditoría puede ser interna o externa, dependiendo de la situación.
- **Seguridad de acceso de terceros:** En esta sección se debe especificar todos los posibles accesos de personas que no pertenecen al staff de trabajadores de la empresa pero que pueden acceder de forma física a las instalaciones de la empresa. Esto puede incluir visitas, proveedores, familiares, etc. Esta descripción puede abarcar los contratos con terceros y su

inclusión a la gestión de riesgos y auditoria de procesos de seguridad.

- **Tercerización:** Se deben describir las políticas y contratos de tercerización en la perspectiva de seguridad de la información; se debe incluir la también a su inclusión a la gestión de riesgos y auditoria de procesos de seguridad de estos servicios.

- **Control de activos:** Para esta área se debe hacer referencia al inventario de activos de información según el área que corresponda.
- **Seguridad en el personal:** esta sección de la política se orienta a las responsabilidades y obligaciones en el factor humano. Para esta área se debe coordinar con el área de recursos humanos y establecer los términos en conjunto. Se debe considerar los siguientes aspectos:
  - **Seguridad en la definición de puestos de trabajo y asignación de recursos:** Esta sección se subdivide en:
    - **Seguridad de los puestos de trabajo:** se deben adicionar las funciones y responsabilidades con respecto a la seguridad al documento de responsabilidades de los puestos.
    - **Controles de personal:** Mencionar que se llevaran a cabo monitoreo de las actividades del personal en temas de seguridad.
    - **Compromiso de confidencialidad:** Se especifica cómo se debe suscribir un compromiso de confidencialidad.
    - **Términos y condiciones de empleo:** Se debe especificar los términos y condiciones considerando la seguridad.
  - **Capacitación al usuario:** Este es un área critica del modelo se seguridad de la información; por lo tanto, se debe considerar la capacitación en temas de seguridad. Además, se debe establecer la obligación de participar en estas capacitaciones. También se debe incluir la periodicidad de las capacitaciones y otros que considere necesarios.
  - **Uso aceptable de tecnología:** se define cual es el uso aceptable de los servicios informáticos, de los equipos y las medidas de seguridad de los empleados adecuadas para proteger los recursos de la empresa y la información confidencial de la organización.

- **Respuesta a incidentes de seguridad:** Esta es un área vital para la gestión de la seguridad y para el mejoramiento del modelo. Se debe considerar:
  - **Comunicación de incidentes de seguridad:** se deben establecer los procedimientos de comunicación en caso suceda un incidente de seguridad.
  - **Comunicación de vulnerabilidades:** se deben establecer los procedimientos de comunicación en caso se encuentren vulnerabilidades y la prohibición de probar dichas fallas a propósito.
  - **Comunicación en fallas de software:** se deben establecer los procedimientos de comunicación si se encuentran fallas en algún tipo de software o sistema operativo.

- **Seguridad física y ambiental:** Se considera el ambiente físico de instalaciones y locaciones en particular. Se debe tener en cuenta:
  - **Identificar el perímetro de seguridad física:** Se deben establecer los componentes perimetrales y relacionados a la seguridad física como rutas de escape y ubicación de extintores. Se debe establecer tipos de áreas y diferenciar entre áreas de acceso público, privado y restringido.
  - **Controles de acceso físico:** Se deben considerar los controles de acceso a personal y gente fuera del ámbito de la empresa. Esto dependerá de la institución y de lo los activos que desea proteger en la misma.
  - **Protección de oficinas e instalaciones:** Se debe detallar las políticas de custodia y acceso de estos ambientes.
  - **Ubicación y protección de equipamiento y copias de seguridad:** En este caso se deben considerar los controles relacionados a este rubro y las políticas relacionadas al manejo de estas.
  - **Suministros de energía:** Se deben establecer las políticas con respecto al uso apropiado de estos suministros, así como de la disponibilidad del mismo y que hacer en caso este fallara.
  - **Seguridad en el cableado:** Se deben establecer los requerimientos mínimos para el cableado y transporte de información en las redes.

- **Mantenimiento de equipos:** Se debe establecer la necesidad de dar mantenimiento a los equipos para asegurar su funcionamiento correcto
- **Uso de equipos fuera de las instalaciones:** se deben establecer los lineamientos de uso de equipos como computadoras, laptops, dispositivos móviles, etc. que pertenezcan a la compañía o pertenezcan a los usuarios, pero sean usados en la compañía.
- **Políticas de escritorios y computadores personales:** Se debe establecer los lineamientos con respecto a documentos privados y su almacenamiento; así como de documentos y archivos importantes en las computadoras personales.
- **Retiro de bienes:** Se establecen las políticas para retirar bienes de la empresa; esto depende de la empresa y su rubro.

- **Comunicaciones y operaciones:** Se deben adoptar medias de protección en la red y también separar las áreas de la empresa, así como y segregar funciones para evitar riesgos de ataques informáticos y de fraude. Se deben considerar los siguientes temas:
  - **Procedimientos y responsabilidades operativas:** Esta área se subdivide en:
    - **Documentación de los procesos operativos:** Se deben documentar los procedimientos de seguridad y de manejo de información.
    - **Control de cambios en operaciones:** Si se realiza un cambio en la documentación anterior debe ser documentado.
    - **Procedimientos de manejo de incidentes:** También se debe establecer la necesidad de la documentación y la gestión de incidentes de seguridad.
    - **Segregación de funciones:** Se debe establecer, tanto para procedimientos como para sistemas la división de funciones del personal y evitar cambios no autorizados y fraudes en la información o sistemas.
    - **Separación entre áreas de desarrollo y operativas:** Si la empresa desarrolla su propio software, debe considerar la separación entre las áreas de desarrollo de software y la de operaciones por razones de seguridad. Se debe establecer esta separación y su descripción.

- **Gestión de instalaciones externas:** Para el caso de tercerización se debe contemplar controles de seguridad con el proveedor del servicio y estos deben aparecer en el contrato; esto se debe especificar en esta área para que todo contrato de tercerización deba contener estos puntos.

- **Planificación y aprobación de sistemas:** Esta área debe tener lo siguiente:
  - **Planificación de la capacidad:** Se debe establecer la necesidad de monitorear la capacidad de operación de los sistemas de la empresa y ser capaces de proyectar las demandas a futuro. Además, se debe incluir que se reporten las necesidades al respecto a las áreas competentes.
  - **Aprobación del sistema:** Se debe especificar la necesidad de plantear criterios de aprobación para los nuevos sistemas. Entre estos puntos se debe considerar: el impacto del desempeño en los equipos de la empresa, recuperación de errores, poner a prueba los procedimientos relacionados al sistema, controles de seguridad, continuidad del negocio, aseguramiento de que el nuevo sistema no afecte los ya instalados, capacitación en el uso del nuevo sistema, entre otros.
- **Protección contra software malicioso:** En esta sección se debe considerar, procedimientos para evitar el ingreso de software malicioso y de concientización a los usuarios. En este apartado se debe considerar:
  - Prohibir software no autorizado.
  - Redacción de procedimientos para evitar obtener software malicioso por cualquier medio.
  - Instalación y actualización de software de detección de virus y examinación de computadores y dispositivos.
  - Mantenimiento de sistemas con actualizaciones de seguridad disponibles y la prueba de las mismas para ver si afectan al sistema con un modo de recuperación y adaptación de los cambios.
  - Revisión periódica de software y datos de equipos de procesamiento en sistemas críticos de la empresa en búsqueda de archivos no autorizados ni aprobados.

- Verificar archivos antes de usarlos en búsqueda de malware en medios electrónicos y redes no confiables.
- Realizar la redacción de procedimientos de verificación de software malicioso según reportes y boletines de seguridad actuales.
- Redactar sobre concientización al personal sobre problemas de ingeniería social y como deben proceder en caso de dudas y ocurrencias.

- **Mantenimiento:** Para el caso del mantenimiento se debe considerar:
  - **Resguardo de la información:** se debe especificar las formas de resguardo de información de acuerdo a la evaluación del activo de información. Se debe considerar rótulos y almacenamiento remoto de copias de seguridad, considerando procedimientos de restauración en respaldo y las pruebas de su efectividad; además se debe considerar procedimientos de destrucción de medios desechados. También se debe considerar resguardo de protección física para los lugares de respaldo.
  - **Registro de actividades del personal operativo:** Se debe considerar un registro de las actividades del personal en sus operaciones. Se deben considerar los tiempos de inicio y cierre de sistemas, errores de sistema y correcciones hechas, intento de acceso al sistema, información crítica y acciones restringidas, ejecución de operaciones críticas y los cambios en ellas. Todo registro de actividades debe quedar registrado.
  - **Registro de fallas:** se debe escribir un registro de fallas y su comunicación oportuna en el proceso de información para su corrección adecuada. Además, se debe tener en cuenta que las correcciones no comprometan la seguridad y por último se debe considerar la documentación de la falla.
  - **Administración de la red:** se deben tener en consideración los controles de redes: se deben especificar los controles en la red interna y externa de la empresa para temas de acceso remoto, controles de transmisión de información por redes

públicas y establecer las pruebas de supervisión de estos controles.

- **Administración y seguridad de los medios de almacenamiento:** para este rubro se debe considerar los siguiente:
  - **Administración de medios informáticos removibles:** se deben establecer procedimientos para el uso de medios informáticos removibles como cintas, discos, memorias extraíbles, casetes, informes impresos, etc. Estos deben contener como eliminar de forma segura contenido si no se utilizará más, Además, se debe establecer un requerimiento de autorización para retirar cualquier medio y considerar un registro de estos; también, el almacenamiento adecuado de los medios informáticos.
  - **Eliminación de medios de información:** se debe considerar la escritura de procedimientos de eliminación de medios como documentos en papel, grabaciones, cintas de impresora, cintas magnéticas, discos o casetes, datos de prueba, documentación organización de la empresa y de sistemas, etc. También se puede tener en cuenta la recolección de estos para su eliminación.
  - **Procedimientos de manejo de información:** Se deben especificar procedimientos para proteger y almacenar información que debe incluir la protección de documentos, redes, sistemas informáticos, comunicaciones móviles, computación móvil, correo electrónico, comunicaciones de voz, multimedia, uso de máquinas de fax y otros sensibles. Además, se debe tener en consideración, restringir el acceso a la información a personal autorizado, considerar un registro formal de los receptores datos, garantizar los datos de entrada, el procesamiento y salida de información, proteger los datos en espera, conservar los medios de almacenamiento en ambientes que los fabricantes o proveedores indiquen.
  - **Seguridad de la documentación de sistema:** se debe tener en cuenta almacenar documentación del sistema de forma

segura y la restricción de esta información al personal autorizado.

- **Intercambios de información y software:** se debe considerar en esta área:
  - **Acuerdos de Intercambio de Información y Software:** Se deben especificar las condiciones de seguridad y de confidencialidad al compartir información o software con otras empresas o proveedores. Estos deben contemplar también registros de envío y recepción de esta información, controles de seguridad, términos y condiciones de uso, y guías de uso correcto.
  - **Seguridad de medios de transito:** debe comprender los procedimientos de transporte de medios informáticos entre diversos puntos. Esto dependerá del valor del activo de información a transportar.
  - **Seguridad en el correo electrónico:** Se deben establecer procedimientos con respecto al uso de correo electrónico institucional que deben contemplar protección de correo electrónico, de archivos adjuntos, uso de técnicas criptográficas (según el valor de la información), retención de mensajes por motivos legales, controles para analizar mensajes electrónicos, aspectos técnicos y operativos de funcionamiento como tamaño de archivos adjuntos, tamaño de buzón de llegada, uso apropiado del correo electrónico, potestad de la empresa de auditar los correos electrónicos dentro de la empresa.
  - **Seguridad de los sistemas electrónicos de oficina:** Se debe considerar el establecimiento de procedimientos en el uso de documentos, computadoras, tecnología móvil, correo, multimedia, etc. dentro de las oficinas.
  - **Sistemas de acceso público:** Se debe tener en consideración el establecimiento de procedimientos que guíen el uso de información sensible considerando la ley de protección de datos personales vigente en el Perú – Ley 29733 u otra ley dependiendo del país.
  - **Otras formas de intercambio de información:** Se debe considerar los lineamientos y procedimientos de cualquier

otro tipo de intercambio de información, dependiendo del rubro de la empresa, teniendo en cuenta la información que se comparte por medios como dispositivos móviles o teléfonos dentro de la empresa y que no deban ser compartidos en lugares públicos.

- **Control de accesos:** El control de los accesos a información es indispensable en la seguridad de la información. Las restricciones y excepciones son necesarias para evitar la pérdida o robo de información y se deben establecer procedimientos formales para asignar acceso al personal desde su incorporación a la empresa hasta su cese de la empresa. En esta área se debe asignar responsabilidades especificas a los responsables de brindar, supervisar, controlar, y revocar acceso a los sistemas de información, en general, el encargado de estos procedimientos es el responsable del área de tecnologías de la información (TI) y sus responsabilidades deben estar especificadas en esta área. Además de esto se debe considerar:
  - **Requerimiento para el control de acceso:** esta área debe considerar los siguientes aspectos:
    - **Política de control de accesos:** esta política estipula aspectos como la identificación de requerimientos de seguridad en las aplicaciones, identificación de la información que se relaciona con las aplicaciones como se considerando el inventario de activos de información, la identificación de leyes aplicables y obligaciones contractuales con respecto a la protección de datos personales (Ley 29733) y servicios relacionados, definición de perfiles de acceso de usuarios estándar y/o comunes a cada puesto de trabajo, la administración de derechos de acceso en un ambiente de red distribuido.
    - **Reglas de control de accesos:** Se debe considerar indicaciones expresas acerca de si las reglas son obligatorias u optativas; además, se debe establecer reglas sobre la premisa “Todo se prohíbe, a menos que se permita expresamente” debido a que es mejor dar acceso que quitarlo si se desconoce la situación. También, se debe controlar los cambios en permisos de usuario si se tiene hace

la asignación automáticamente o si lo hace el administrador del sistema.

- **Administración de acceso a usuarios:** la gestión de acceso a usuarios debe estar especificada de la siguiente manera:
  - **Registro de usuarios:** se debe especificar que el responsable de seguridad debe especificar el procedimiento de registro de usuarios que debe contener:
    - Identificación de usuario.
    - Verificación de usuarios.
    - Verificación de nivel de acceso.
    - Entrega de derechos de acceso al usuario.
    - Requerimiento de aceptaciones de condiciones de uso firmadas por los usuarios.
    - Garantizar que los accesos no estén disponibles hasta que no se completen los procedimientos de autorización de registro.
    - Mantener un registro de usuarios registrados activos e inactivos.
    - Cancelación de accesos en caso de cambio de acceso, perdida de credenciales, o cese de labores.
    - Revisiones periódicas de los accesos
    - Incluir cláusulas en los contratos que especifiquen sanciones en caso de acceso no autorizado.
  - **Administración de privilegios:** se debe indicar la necesidad de estipular los privilegios en los sistemas operativos, bases de datos, aplicaciones, considerando la base de necesidad de uso y necesidad de saber de información. Además, se debe establecer la necesidad de implementación de los privilegios de acceso en los sistemas implementados. También, se debe establecer un tiempo determinado de vigencia para los privilegios de acceso. Por último, se debe especificar la necesidad de desarrollar sistemas que contemplen niveles de acceso y privilegios.
  - **Administración de contraseñas de usuario:** se debe establecer la administración formal de contraseñas para los usuarios ; se debe tener en consideración: el requerimiento

de una declaración formal expresa que comprometa a los usuarios a mantener su contraseñas en completo secreto, que obligue el cambie el cambio de contraseñas en un lapso de tiempo, almacenamiento de contraseñas en sistemas informáticos seguros, se recomienda de forma encriptada, utilización de otras tecnologías de autenticación de tipo biométrico dependiendo del activo de información en cuestión, especificación del formato de contraseñas que contengan cantidad mínima de caracteres y uso de caracteres especiales y mayúsculas, bloqueo en casos de ingreso fallido, solicitud de contraseña, impedimento de que se reutilicen contraseñas antiguas, caducidad de contraseñas, según sea el caso, etc.

- **Revisión de derechos de acceso a usuarios:** se debe fijar supervisiones a los derechos de acceso de usuarios en un periodo de tiempo, accesos especiales, y la asignación de privilegios.

- **Responsabilidades de usuario:** se debe especificar también la responsabilidad de usuario considerando lo siguiente:
  - **Uso de contraseña:** Se debe especificar las buenas prácticas para la selección y manejo de contraseñas de los usuarios considerando que se mantengan las contraseñas en secreto, solicitar cambio de contraseña, seleccionar contraseñas de calidad, cambio de contraseñas, no guardar contraseñas automáticamente, entre otros.
  - **Equipos desatendidos en áreas de usuarios:** Se debe exigir el cierre de sesión de los usuarios cuando dejen sus estaciones de trabajo, se debe proteger con contraseña el cierre de sesión.
- **Control de accesos a la red:** Se debe considerar el control del acceso a la red en los siguientes aspectos:
  - **Política de uso de servicios de red:** El área de informática debe determinar el acceso a la red identificando las redes y servicios disponibles en la red para realizar las normas y procedimientos y considerando los controles que se deben considerar.

- **Rutas establecidas:** se deben establecer rutas de comunicación de red bien definidas para los sistemas de red limitando el acceso a la red cuando no sea necesario.
- **Autenticación de usuarios en redes externas:** Se deben establecer los lineamientos para el acceso de los usuarios en redes externas considerando una autenticación de doble factor como mínimo (contraseña y otro como token, mensaje telefónico). Además, se debe incluir los procedimientos de implementación de autenticación en los sistemas para estos casos.
- **Protección de puertos de diagnóstico remoto:** se debe estipular el bloqueo de puertos que no sean necesarios para la conexión y diagnóstico de redes.
- **Subdivisión de redes:** Se debe estipular la necesidad de la segmentación de redes y subredes utilizando dominios y considerando la política de control de accesos a la red.
- **Acceso a internet:** el acceso a internet debe estar controlado y restringido a las necesidades del negocio; por lo tanto, se debe implementar un filtro de internet adecuado, firewall, proxy u otras tecnologías que protejan a la empresa de intromisiones externas. En el caso de requerir algún acceso adicional, este debe tener una autorización formal.
- **Control de conexión de red:** Se debe considerar la limitación de acceso a ciertos entornos considerando los niveles de acceso de los usuarios.
- **Seguridad de los servicios de red:** Se debe establecer los controles en la red donde se tengan sólo los servicios que se utilicen, se controle el acceso lógico de servicios, configurando lo servicio de manera seguro según las mejores prácticas e instalando las actualizaciones de seguridad. Para esto el responsable de seguridad y responsable del área de TI deben coordinar estos controles.

- **Control de acceso al sistema operativo:** se deben considerar los siguientes puntos.
  - **Control de acceso de usuarios:** Se deben establecer los lineamientos para la protección del sistema operativo considerando la identificación y autenticación de usuarios y

uso adecuado de contraseñas que consideren buenas prácticas.

- **Uso de utilitarios de sistema:** se deben establecer los lineamientos de uso de utilitarios para sistemas operativos y diferenciarlos con los de software; así como teniendo un registro de estos en consideración con los niveles de acceso.
- **Alarmas silenciosas para la protección de los usuarios:** Se podría incluir alarmas silenciosas para evitar coerciones a los trabajadores.
- **Desconexión de terminales en tiempo muerto:** Se debe considerar la desconexión de los terminales luego de un tiempo establecido como una actividad recomendada para evitar intrusiones no deseadas.
- **Limitación del horario de conexión:** se debe contemplar establecer límites de acceso a los sistemas para horarios establecidos. Esto aplicará a sistemas con acceso en la empresa y tal vez con acceso remoto.

- **Control de acceso a aplicaciones:** Con respecto a las aplicaciones se debe considerar:
  - **Restricción de acceso a la información:** Se deben considerar controles que restrinjan el acceso a información considerando niveles de acceso; se debe considerar una interfaz apropiada para usuarios según niveles de acceso, controlar derechos de acceso del personal según el uso de la información que se tenga (lectura, escritura, eliminación). Además, se debe garantizar que sólo se muestre información necesaria, sobre todo con datos sensibles y se debe restringir la información que no se necesite usar.
  - **Aislamiento de sistemas sensibles:** Se debe considerar establecer un ambiente adecuado para tratar sistemas que sean sensibles o que puedan originar pérdidas considerables. Se debe considerar el encargado de dicho sistema, así como los controles que se implementarán.
- **Monitoreo de acceso y uso de sistemas:** el uso de los sistemas debe ser monitoreado considerando diversos factores:
  - **Registro de eventos:** Se deben tener registros de auditoría que deben incluir identificación de usuario, fecha y hora de

inicio y fin de sesión, identificación y ubicación de terminal, registros de intentos exitosos y fallidos de acceso al sistema y de acceso a datos y otros recursos.

- **Monitoreo de uso de sistemas:** Se deben incluir los siguientes aspectos:
  - **Procedimientos:** Se debe implementar monitoreo del desempeño correcto del personal y para esto se debe tener en cuenta:
    - **Acceso no autorizado:** que incluye, identificación de usuario, fecha y hora de evento, tipo de eventos, archivos a los que se accede, utilitarios y programas utilizados.
    - **Operaciones con privilegio**: por ejemplo, utilización de cuenta de supervisor, inicio y cierre de sistema, cambio de fecha y hora, cambios en configuración de seguridad, alta de servicios, etc.
    - **Intentos de acceso no autorizado:** esto debe contemplar intentos fallidos, violaciones a la política de accesos, alertas de sistema de detección de intrusos, si se tiene una implementada.
    - **Alertas o fallas de sistema:** se consideran alertas de consola, excepciones de sistema de registro, alarmas de administración de redes, accesos remotos a los sistemas.
  - **Registro y revisión de eventos:** Se debe implementar un procedimiento de registro y revisión de los registros de auditoría para poder generar informes de amenazas y riesgos detectados; además, se deben considerar medidas de protección para que estos registros no sean modificados de ninguna manera.
  - **Sincronización de relojes:** Se debe considerar la sincronización de relojes por cuestiones de tener registros correctos de auditoría.

- **Computación móvil y trabajo remoto:** En la nueva tendencia de trabajo, se pueden considerar aspectos de dispositivos móviles y de teletrabajo, por lo tanto, se debe considerar estos aspectos si la empresa hace uso de ellos:

        - **Computación móvil:** Si se hace uso de tecnologías móviles, se debe contemplar todas las medidas de seguridad como por ejemplo acceso seguro, protección de dispositivos, técnicas de encriptación, protección de software malicioso, etc. además, de esto se debe establecer ciertas indicaciones sobre los dispositivos que se usan como custodiar los dispositivos, no llamar la atención a ellos, no usar logotipos de la empresa en ellos, no poner datos de contacto y mantener información clasificada de forma cifrada.
        - **Trabajo remoto:** Se debe considerar las normativas de teletrabajo si es que se diera el caso y también considerando los controles de seguridad necesarios para acceso remoto.
- **Desarrollo y mantenimiento de sistemas:** se debe considerar que el desarrollo de nuevos sistemas dentro de la empresa y su mantenimiento deben contener controles adecuados.
    - **Requerimientos de seguridad de los sistemas:** Se debe considerar un procedimiento por etapas para la protección de los sistemas, también se debe considerar el factor económico de proteger los sistemas en vista del valor del activo. Para el caso de nuevos sistemas, se puede considerar la implementación de controles desde el diseño, puesto que es más costosa una implementación posterior.
    - **Seguridad en los sistemas de aplicación:** se requiere que los sistemas de aplicación tengan controles como la validación de datos de entrada, el procesamiento interno, interfaces entre sistemas y la validación de datos de salida, todo esto considerando las buenas prácticas de programación y desarrollo de sistemas.
    - **Controles criptográficos:** Se deben considerar controles criptográficos en los sistemas y almacenamiento de información valiosa considerando los siguientes aspectos:
        - **Política de uso de controles criptográficos:** se debe considerar el uso de controles criptográficos de acuerdo a las últimas formas de control criptográfico y dependiendo del uso de lo que se desea encriptar y para qué. Sin embargo, se recomienda utilizar encriptación de 256 bits simétrico y asimétrico. Asimismo, se debe considerar el uso de firmas

digitales y controles de cifrado para el envío de información importante y el uso de claves apropiadas. Además, se deben considerar normas, procedimientos y métodos de uso de claves y controles criptográficos considerando las mejores prácticas en este tema.

- **Seguridad de los archivos de sistema:** Se deben tener en cuenta todas las disposiciones que garanticen que las actividades de soporte de los sistemas se hagan de forma controlada. Se deben considerar los siguientes puntos:
  - **Control de software operativo:** Se debe considerar que el área operativa no puede servir como ambiente de pruebas para el área de desarrollo; por eso, se debe tener en consideración un sólo implementador de software en el área de desarrollo, disponiendo la división entre área operativa y área de producción de software, se debe considerar la implementación sin afectar otras áreas de la empresa, su aceptación será posterior a las pruebas. Además, se debe mantener un registro de las actualizaciones realizadas, debiendo también retener las versiones anteriores en caso de fallos. También se debe definir un procedimiento que establezca el proceso de actualizaciones, las pruebas, etc. Por último, se debe evitar que el implementador se involucre en el área de desarrollo o mantenimiento (Segregación de funciones).
  - **Protección de los datos de prueba del sistema:** para las pruebas, se debe establecer que las bases de datos operativas jamás pueden ser utilizadas en pruebas; también, se debe solicitar realizar una copia de la base de datos; se recomienda utilizar información no real para las pruebas. Al final de las pruebas, se debe destruir esta información siempre.
  - **Control de cambios a datos operativos:** Para el caso de cambios y eliminación de datos operativos, es necesario utilizar el control de accesos como línea base; sin embargo, en casos excepcionales será el responsable de seguridad de la información quien dicte las pautas para estos procesos.

- **Control de acceso a las bibliotecas de programas fuente:** Se debe establecer una biblioteca de programas fuente como respaldo para los sistemas de la empresa. El acceso a esta biblioteca debe tener autorización del responsable de TI, además, se debe tener un registro de los programas fuente en uso; también se debe asegurar que se tengan diversas versiones de los programas fuente y que un mismo programa no sea modificado por más de un desarrollador. También se debe considerar que el administrador de los programas fuente no modifique ningún programa a su cargo.

- **Seguridad de los procesos de desarrollo y soporte:** se debe considerar lo siguiente:
  - **Procedimiento de control de cambios:** para todo cambio en los sistemas de información se debe tener autorización de los jefes de área afectados para que se informe a sus áreas respectivas. Se debe tener un registro de cambios a los sistemas que sea acorde con el registro de segregación de funciones. Además, se necesita tener un respaldo del sistema en caso de fallo: también es necesario actualizar la documentación. Asimismo, debe ser el implementador quien efectué los cambios en los sistemas.
  - **Revisión técnica de cambios de sistema operativo:** en base a los cambios que se realicen, se debe determinar si es necesario un cambio de sistema operativo considerando que esto no afecte a los sistemas del área de operación.
  - **Restricción de cambios de paquetes de software:** Se debe considerar aspectos relacionados a cuidar software que ingresa a la empresa adquiriendo software de proveedores acreditados o de productos ya evaluados; se debe evaluar el código fuente cuando se pueda, controlar la modificación de código instalado y la utilización de herramientas para la protección contra código malicioso.
  - **Desarrollo externo de software:** si se desarrolla software fuera de la empresa, se necesita considerar: acuerdo de licencia, derecho de código, entre otros. Además, se necesitan acuerdos de calidad, mantenimiento, custodia de

programas fuente, y la inclusión de auditoria como parte de los contratos.

- **Administración de la continuidad de las actividades del organismo:** El proceso de continuidad de negocio es necesario para toda empresa, puesto que, ante una eventualidad de nivel catastrófico, si no se tiene un plan de continuidad de negocio, lo más probable es que el negocio termine. Por lo tanto, el responsable de la seguridad de la información determinará el plan de continuidad considerando lo siguiente:
  - **Proceso de la administración de la continuidad de negocios:** Para este tipo se debe considerar identificar y dar prioridad a los procesos críticos de la empresa; es vital que la gerencia entienda lo que conllevaría no asegurar los procesos críticos; luego de esto se debe elaborar y documentar la estrategia de continuidad de negocio para luego proponer el plan para la implementación de la estrategia. Luego de la aprobación del plan, se deben establecer cronogramas para pruebas del plan y su actualización periódica.
- **Cumplimiento:** Todo las políticas y procedimientos deben ser normados por el área legal. Por lo tanto, en coordinación con el área legal de la empresa, se deben establecer ciertos aspectos de cumplimiento:
  - **Cumplimiento de los requisitos legales:** Aquí se debe considerar los siguiente:
    - **Identificación de la legislación aplicable:** Se debe hacer una revisión de la legislación local y nacional; en consideración de la obligación de la ley, se debe alinear cada control a lo que establece la ley.
    - **Derechos de propiedad intelectual:** Se debe considerar la legislación actual con respecto a la propiedad intelectual, leyes de marcas y patentes y las disposiciones de instituciones como INDECOPI, en el caso de Perú.
    - **Protección de registro de la empresa:** Se debe considerar protección adicional a registros e información sensible existente en las empresas. Estos registros podrán ser clasificados como registros de base de datos, registros contables, registros de procedimientos operativos, registros de auditoría, entre otros detallando el tiempo en que deben

ser retenidos y los medios en que se almacenarán como papel, medios ópticos o magnéticos, microfichas, etc.

- **Protección de datos personales:** cada empleado de la empresa debe conocer los límites y restricciones en el uso de información sensible. Para esto, la empresa debe requerir un compromiso de confidencialidad firmado y que debe ser retenido por la empresa. La ley actual en el Perú es la ley 29733.
- **Prevención de uso inadecuado de los recursos de procesamiento de información:** Se debe establecer que todos los recursos que procesan información en la empresa debe ser utilizados con un propósito definido. Si existe otro uso que no sea el autorizado, se considerará ilegal.
- **Regulación de controles para firmas y certificados digitales:** Se debe establecer la necesidad de considerar la ley 27269 en el Perú para el uso de firmas y certificados digitales en los sistemas.
- **Recolección de evidencia:** Se recomienda establecer los lineamientos para el recojo de evidencia; en el caso se encuentre a una persona actuando en contra de la empresa y la política de seguridad, se debe tener la evidencia necesaria para acciones disciplinarias. Por supuesto, si el problema trasciende a ámbitos legales, se debe contar con evidencia conforme a la ley; para eso se debe coordinar con el área legal de la empresa para poder dar tratamiento correcto a la evidencia.

- **Revisiones de la política de seguridad y la compatibilidad técnica:** la política de seguridad no es un documento perenne, sino que debe ser revísalo y actualizado; se debe considerar lo siguiente en esta área:
  - **Cumplimiento de la política de seguridad:** se debe especificar que el responsable de cada área de la empresa debe velar por el cumplimiento de las políticas de seguridad de su área; además el responsable de la seguridad de la información supervisará periódicamente como se cumplen las políticas en las áreas como segunda medida de implementación.

- **Verificación de la compatibilidad técnica:** se establecerá que el responsable de la seguridad de la información revisará el cumplimiento de las políticas en los sistemas de información en términos de hardware y software, se recomienda la asistencia técnica especializada para este proceso. Se considerarán pruebas de penetración para tratar de conseguir vulnerabilidades y para poner a prueba la eficacia de los controles. Se recomienda la contrata de un hacker ético para esta tarea.
- **Consideraciones de auditoria:** Se debe estipular la realización de auditorías internas y externas con la finalidad de descubrir riesgos no considerados anteriormente; se deben tomar estas auditorías como una oportunidad de crecimiento.
- **Sanciones previstas por incumplimiento:** se debe especificar las sanciones a los que no acaten las dispersiones de la política y estas dependerán de cómo la empresa quiere manejar las ocurrencias y considerará la gravedad de las mismas según su criterio.

El modelo de política presentado, puede variar según el alcance de la empresa, sin embargo, se recomienda tratar de poner en práctica aquellas secciones que sean de relevancia para la empresa y que describan procesos críticos de seguridad. Si se desea mayor referencia, se puede consultar el (ISO/IEC 27002, 2013). Ahora bien, antes de dar a conocer las políticas de seguridad de la información, es importante tener la aprobación de gerencia y de los departamentos involucrados; por lo tanto, se necesita brindar una copia de evaluación a los stakeholders; luego de considerar las sugerencias que no comprometan la seguridad de la información en la empresa, se debe tener la versión final de la política de seguridad de la información y esta debe ser aprobada por la gerencia de la empresa. Además, se debe preparar un plan de implementación de las políticas y un plan de implementación gradual de controles tecnológicos que conllevará a elaborar un presupuesto de implementación tecnológico por etapas que considere el uso de tecnologías de uso libre o de compra, dependiendo del nivel de gasto de la empresa y al nivel de protección que

se desee tener en los activos de la información. Los planes mencionados deben ser presentados a gerencia para su estudio y aceptación final.

Luego de haber tener por escrito la política de seguridad de la información para la empresa, se necesitan establecer los procedimientos e instructivos para todas las políticas que lo requieran; por supuesto, esto debe ser parte del plan del plan de implementación gradual de las políticas y controles. Teniendo la política y conociendo ya los controles que se deben implementar, se debe pasar a la fase de dar a conocer las políticas al personal de la compañía.

4.4.2.7 Fase 7: Dar a conocer la política de seguridad de la información

Una vez aprobada la política de seguridad de la información, el siguiente paso es dar a conocer la política de seguridad al personal de la empresa. Ahora bien, el dar a conocer las políticas no es simplemente una distribución masiva a todo el personal; este proceso involucra una serie de actividades que ayuden a maximizar el alcance de conocimiento que se pueda tener con el documento; además, la presentación de la misma no es suficiente, se necesita un trabajo que continúa de la fase de conocer al personal y también se requiere el apoyo de la gerencia general y la gerencia de recursos humanos, así como de las jefaturas o gerencias de cada departamento de la empresa. Por lo tanto, para dar a conocer las políticas de seguridad de la información, se necesitan lo siguientes pasos:

- En primer lugar, se debe asegurar que el documento se haga público en cada área de trabajo de la empresa. Para eso se debe coordinar una reunión general con los jefes de departamento de la empresa y se debe dar a conocer cuán ventajosa y necesaria es la implementación de la política en la empresa. Para esto se debe preparar una presentación ejecutiva de lo que contempla la política de seguridad de la información de forma general y sucinta y siempre enfocada en los beneficios del de la misma y los aspectos que se necesitará afectar.
- Luego de tener como parte de apoyo a los jefes de departamento, se necesita una reunión con todos los demás empleados para dar a conocer las políticas de seguridad, sus ventajas y la forma en cómo se implementará de forma general. Se recomienda que se presente esta información en un ambiente agradable y que de algún pequeño

beneficio al personal como un desayuno, almuerzo o cena donde se disponga de la información de manera familiar, pues se tendrá una mejor recepción de la información nueva.

- Habiendo comunicado las políticas de seguridad de la información a todo el personal, se debe elaborar un cronograma de capacitaciones para cada área en particular con todos los involucrados. Para esto se necesita coordinar con cada jefe de departamento para establecer las fechas respectivas y preparar un cronograma de capacitaciones por cada área.
- Cada capacitación necesita orientarse al éxito de la gestión en su conjunto y al mismo tiempo debe brindar las pautas para dar cumplimiento a las políticas a nivel personal, a nivel de área y a nivel organizacional. Se recomienda tener en cuenta los siguientes puntos en las capacitaciones:
    - Brindar el propósito de la capacitación.
    - Dar a conocer los objetivos del modelo y de la política.
    - Brindar pautas de seguridad de información personal. Este es el núcleo de la cultura y comunidad de seguridad de la información.
    - Establecer la necesidad de generar una cultura de seguridad de la información.
    - Brindar información de la política con respecto al área en particular y que se relaciona con toda la empresa.
    - Especificar responsabilidades, obligaciones y sanciones respecto al cumplimiento de la política de seguridad de la información.
    - Aclarar preguntas al respecto y brindar información de contacto en caso de dudas. Se debe enfatizar ante cualquier duda que se puede consultar sin ningún temor o reserva.

- Se recomienda también tener una copia de la política de seguridad de la información en la jefatura de cada área de la empresa para que el personal en estas áreas pueda revisarla cuando la requieran; además, se recomienda tener una versión digital del área pertinente que debe ser distribuida por secciones luego de la reunión con todos los trabajadores. Además, se recomienda, utilizar anuncios cortos y posters que contengan puntos claves de la seguridad de la información de forma constante por medio de correo o en físico en los boletines de anuncios o lugares visibles para que se vaya generando

un estado de cultura de seguridad de la información que todos puedan compartir.

Como último paso, se requiere dar una fecha de inicio de aplicación de la política de seguridad y comenzar con la ejecución de la misma. Posteriormente a esto, se debe dar tratamiento al factor humano en la seguridad de la información.

4.4.2.8 Fase 8: Dar tratamiento al factor humano

Una vez que las políticas de la información estén en pleno despliegue y ejecución, es necesario seguir fortaleciendo el factor humano. Si bien es cierto, se comenzó a fortalecer el factor humano en el conocimiento del personal y ya se están llevando a cabo capacitaciones orientadas a fortalecer valores que son necesarios para incrementar el nivel de cultura de seguridad de la información, pero aún se puede hacer algo más. Es necesario ahora generar una cultura de seguridad de la información basada en aspectos individuales y de grupo. Para lo cual, teniendo en cuenta las teorías de comportamiento humano como la teoría de comportamiento planificado (Martín, Manuel y Rojas, 2011) y (Cortés, 2001), teoría de necesidades básicas (Clonninger 2002) y teoría de control social (Hirschi, 2003), (Chriss, 2007), (López, 2014), (Hawkins y Weis, 1995) y (Lee, Lee y Yoo, 2004) se puede considerar ciertas medidas para fortalecer el nivel de cultura de seguridad de la información, entre ellas tenemos:

- En primer lugar se sugiere trabajar en los individuos y en temas de su seguridad personal; para esto se pueden brindar charlas, capacitaciones, cursos de seguridad personal y talleres donde se vaya formando una conciencia de seguridad de la información individual; a esto se puede añadir pruebas de desempeño en situaciones simuladas y también evaluaciones de conocimiento que pueden formar parte de la evaluación de desempeño del personal y que permitan añadir puntos adicionales en su evaluación o quizá brindar incentivos para los trabajadores con el mejor desempeño. Esto ayudará personalmente a motivar al personal y servirá como refuerzo positivo en la formación de un comportamiento planificado.

- Paralelamente, se debe trabajar con los equipos de trabajadores. Se puede dividir al personal en equipos de trabajo según área de la empresa o teniendo más equipos dentro de un área; luego se propondrá retos de cultura de seguridad donde cada miembro del equipo debe animar y compartir información de seguridad de la información. De este modo, se evaluará también el desempeño de los equipos en pruebas simuladas de seguridad de la información, brindándoles beneficios por su esfuerzo.
- Luego de esto se puede brindar la retroalimentación necesaria para cada uno de los casos que permita que los trabajadores no se sientan intimidados por despidos repentinos por estos entrenamientos. Al contrario, el objetivo es que cada empleado se sienta seguro de su puesto de trabajo por hacer las cosas bien. Sin embargo, es necesario corregir actitudes que no ayuden o formen una comunidad de seguridad de la información inestable. Esto lo determinará el área de recursos humanos según las políticas de seguridad de la información.
- Además, se puede dar charlas de comportamiento deseado y adecuado en casos de incidentes de seguridad. También, se puede simular ciertas actividades "ilícitas" controladas para poder apreciar la reacción del personal. Si sucediera el caso de que se encontrara a alguna persona accediendo a algún procedimiento ilegal, y está dentro de los parámetros de simulacro, esto puede servir como ejemplo a otros trabajadores, por supuesto tratando de mantener los nombres en reserva; esto puede funcionar como un filtro de personal donde se debe poner atención.
- Con respecto a los beneficios se deben considerar beneficios directamente económicos, días libres, reconocimiento público, también de estudio y capacitación, de crecimiento personal, etc. que puedan motivar de forma externa a los trabajadores a tener un comportamiento orientado a la seguridad de la información individual y grupal.
- Se debe incluir también pruebas de ingeniería social con ayuda profesional especializada en hacking ético para poder probar la fortaleza del personal de forma individual y en grupo. Esto, como parte de la política de seguridad de la información, puede ser usado como

base para brindar capacitaciones focalizadas en temas donde se encuentre debilidad.

- Se debe tratar de generar cultura de seguridad de la información en cada aspecto de la empresa y para esto se puede incluir imágenes, videos, música, etc. que fomenten la seguridad de forma directa o indirecta. El objetivo es que el personal se sienta identificado con su seguridad y el de la empresa.

Lo importante del tratamiento del factor humano es que se realicen actividades que fomenten el crecimiento y fortalecimiento del sistema como un todo y como muchos individuos interrelacionados. Si se trata de forma eficiente el factor humano, no sólo se tendrá un modelo de seguridad bastante robusto, sino también se fomentará una actitud de lealtad y trabajo en equipo que redundará en mayor producción de la empresa. Ahora se necesita ver cuán efectivo es el modelo.

4.4.2.9 Fase 9: Evaluar y revisar

Considerando el trabajo con el factor humano, es necesario evaluar el modelo de seguridad en términos de riesgos, controles, seguridad en el personal y cumplimiento de políticas. Para esto se debe diseñar diversas formas de evaluación para cada una de las áreas en cuestión. Entre las evaluaciones que se deben considerar se tienen:

- Para el área de riesgos y controles, se deben monitorear los controles implementados y se deben realizar pruebas periódicas a todos y cada uno de los controles para ver su rendimiento. Según la prueba, se requiere de personal del área de TI para poder realizar estas pruebas. También se puede contar con el apoyo de un hacker ético para poder encontrar vulnerabilidades en sistemas específicos.
- Para evaluar el personal se puede realizar evaluaciones periódicas de conocimiento sobre políticas de seguridad de la información como se explicó en la fase 8; además, se pueden realizar estudios estadísticos descriptivos sobre la percepción de seguridad de la información en el personal que también considere información sobre conocimiento específico de seguridad. Los resultados pueden ser utilizados para la mejora del modelo de seguridad. Así también, se pueden realizar supervisiones programadas e inopinadas para poder ver el

cumplimiento de las políticas de seguridad tal como lo estipula la política de seguridad de la información.

- Otra manera de evaluar la seguridad de la información es realizar auditorías internas y externas en búsqueda de riesgos que puedan comprometer la seguridad de la información; además, esta auditorias puede servir para mejorar y corregir aspectos referentes a los controles, uso de tecnología, recursos materiales y humanos, etc. Siempre debe tenerse la óptica de mejora continua en el modelo de seguridad de la información.

La evaluación debe ser siempre considerada la forma de mejorar el modelo de seguridad de la información. Para lo cual se requieren indicadores claros de lo que se requiere y plantearse metas respecto a estos resultados tanto en el gobierno como la gestión de seguridad de la información. Además, se debe presentar todo resultado y probabilidad de mejora a la gerencia como parte de la evidencia de la efectividad de la gestión de la seguridad por medio del modelo orientado al factor humano. Como anexo, se presenta una lista de indicadores necesarios para para la evaluación del modelo.

4.4.2.10 Fase 10: Mejorar

El modelo de seguridad de la información nos orienta a buscar una mejora progresiva y continua de la seguridad de la información por medio de la evaluación y revisión para determinar los puntos que se deben mejorar. Para esto se recomienda seguir todas las fases y establecer cambios de ser necesario para tener una gestión de la seguridad cada vez más óptima. Por lo cual se debe empezar a hacer ajustes y mejoras en cada una de las fases del modelo.

4.4.3 Glosario de términos del modelo

Activo

(Inglés: Asset). En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización (The International Organization for Standardization, 2016).

Amenaza

(Inglés: Threat). Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización (The International Organization for Standardization, 2016).

Árbol normativo

Conjunto de documentos que contienen políticas, procedimientos, instructivos y registros.

Conciencia de seguridad de la información

Se define como la facilidad para pensar habitual-mente, en como eliminar riesgos de seguridad de la información producto del trabajo que se encuentran presentes en las tareas que normalmente realizamos (The International Organization for Standardization, 2016).

Confidencialidad

(Inglés: Confidentiality). Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados (The International Organization for Standardization, 2016).

Control

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo (The International Organization for Standardization, 2016).

Cultura de la seguridad de la información

La Cultura de Seguridad es la combinación de los valores, actitudes, competencias y modos de comportamiento, tanto individuales como de grupo, que determinan el compromiso, modelo y competencia de la gestión de la seguridad en la organización. (The International Organization for Standardization, 2016).

Datos sensibles

Es aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales, la información relativa a la salud física o mental u otras análogas que afecten su intimidad (Gobierno/Perú, 2012).

Disponibilidad

(Inglés: Availability). Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada (The International Organization for Standardization, 2016).

Incidente de seguridad de la información

(Inglés: Information security incident). Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (The International Organization for Standardization, 2016).

Ingeniería social

Conjunto de técnicas que a través del engaño obtienen información de una empresa directamente de los trabajadores de esta.

Integridad

(Inglés: Integrity). Propiedad de la información relativa a su exactitud y completitud (The International Organization for Standardization, 2016).

Malware / software malicioso

Software dañino, existen virus, troyanos, gusanos, etc.

Mejora continua

Concepto planteado por Deming en su modelo de calidad para negocios.

Política de seguridad de la información

Documento de que contiene políticas o normas relacionadas con la seguridad de la información y son de ejecución obligatoria (The International Organization for Standardization, 2016)..

Riesgo

(Inglés: Risk). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (The International Organization for Standardization, 2016).

Segregación de funciones

(Inglés: Segregation of duties). Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia (The International Organization for Standardization, 2016)..

Seguridad de la información

(Inglés: Information security). Preservación de la confidencialidad, integridad y disponibilidad de la información (The International Organization for Standardization, 2016).

Stakeholder

(Inglés: Interested party / Stakeholder). Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad (The International Organization for Standardization, 2016).

Vulnerabilidad

(Inglés: Vulnerability). Debilidad de un activo o control que puede ser explotada por una o más amenazas (The International Organization for Standardization, 2016).

4.4.4 Costo de implementación del modelo

El costo de implementación del modelo dependerá del alcance del gobierno de seguridad de la información que se determine la alta dirección, de los controles que desee utilizar para proteger sus activos, de canto desee fortalecer su factor humano, de las tecnologías de seguridad que desee implementar, del nivel de riesgo aceptable para la empresa, entre otras consideraciones que determinan los costos tecnológicos, de gestión y humanos relacionados al modelo. Por lo cual se sugiere que los interesados en la implementación parcial o total del modelo de seguridad de la información, deben evaluar sus costos dependiendo de los factores descritos y relativos a su propia condición.

CONCLUSIONES

1. El ICPNA RC debería invertir en su seguridad de la información y ayudar a sus trabajadores a adquirir conocimiento y hábitos de seguridad de la información. Asimismo, debería implementar el modelo realizado con este fin.

2. Las teorías de comportamiento humano y los estándares de seguridad utilizados para la elaboración del modelo se acoplan de forma coherente porque el tratamiento factor humano debe ser parte de la gestión de seguridad de la información dentro de la institución

3. Aun cuando el modelo se derivó del estudio al ICPNA RC y considera estándares internacionales, se requiere que el modelo sea implantado para poder medir su efectividad tanto en la seguridad de la información de la organización, así como el fortalecimiento de la cultura de seguridad de la información; lo cual no está en el alcance de este estudio.

4. Este modelo de seguridad de la información podría ser implantado en otras organizaciones debido a que considera aspectos de estándares internacionales y describe aspectos transversales a otras empresas, organizaciones e instituciones.

RECOMENDACIONES

1. Se recomienda la implementación del modelo de seguridad de la información propuesto en el ICPNA RC debido a que ayudará a fortalecer el factor humano de la seguridad de la información que ha demostrado ser uno de los problemas más críticos dentro de la seguridad de la información.

2. Se recomienda realizar estudios futuros de mejora en términos de gestión de recursos humanos en la institución luego de la implementación del modelo de seguridad de la información debido a que el modelo propuesto contempla también la mejora del ambiente laboral para aumentar las probabilidades de éxito del modelo.

3. Se recomienda una documentación organizada en cada una de las fases del modelo. Es importante llevar la implementación del modelo de forma ordenada para fines de auditoría y para permitir que la gestión de seguridad de la información a través del modelo sea más fácil de implementar, medir y mejorar.

4. Se recomienda realizar un estudio posterior relacionado al factor humano dentro de otras empresas que ya cuentan con una gestión de seguridad de la información en el país para luego implementar parte o la totalidad del modelo de seguridad de la información propuesto y ver los resultados en términos de fortalecimiento del factor humano de la seguridad de la información.

REFERENCIAS BIBLIOGRÁFICAS

ACHIARY, C., 2005. Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional. . S.l.:

AGUILAR, A., 2014. Estudio cualitativo de las variables para el Uso de las Tecnologías de la Información y las comunicaciones (TIC), por las empresas del segmento MYPE. . Lima, Perú:

AJZEN, I., 1991. The theory of planned behavior. *Orgnizational Behavior and Human Decision Processes*, vol. 50, pp. 179-211. ISSN 07495978. DOI 10.1016/0749-5978(91)90020-T.

AL-MUKAHAL, H.M. y ALSHARE, K., 2015. An examination of factors that influence the number of information security policy violations in Qatari organizations. *Information and Computer Security* [en línea], vol. 23, no. 1, pp. 102-118. ISSN 2056-4961. DOI 10.1108/ICS-03-2014-0018. Disponible en: http://dx.doi.org/10.1108/ICS-03-2014-0018%5Cnhttp://www.emeraldinsight.com/doi/abs/10.1108/ICS-03-2014-0018.

AMPUERO CHANG, C.E., 2011. *Diseño De Un Sistema De Gestión De Seguridad De Información Para Una Campañia De Seguros* [en línea]. S.l.: PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ. Disponible en: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/933/AMPUERO_CHANG_CARLOS_INFORMACION_COMPA?IA_SEGUROS.pdf?sequence=1.

AMUTIO GÓMEZ, M.A., 2012. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. , pp. 127.

ARBAIZA FERMINI, L., 2010. *Comportamiento organizacional : bases y fundamentos*. Original. Buenos Aires: Cengage Learning. ISBN 9789871486304.

BELOCH, C., 2011. Las Tecnologías de la Información y Comunicación (T.I.C.). . Valencia, España:

CAMERON, R., 2012. AJZEN'S THEORY OF PLANNED BEHAVIOR AND SOCIAL MEDIA Ajzen's Theory of Planned Behavior and Social Media Use by College Students. *AMERICAN JOURNAL OF PSYCHOLOGICAL RESEARCH*, vol. 8, no. 1.

CANTERA LÓPEZ, F.J., 1986. *NTP 213: Satisfacción laboral: encuesta de evaluación*. 1986.

Madrid: Gobierno de España.

CHRISS, J.J., 2007. The functions of the social bond. *Sociological Quarterly*, vol. 48, no. 4, pp. 689-712. ISSN 00380253. DOI 10.1111/j.1533-8525.2007.00097.x.

CLONNINGER, S., 2002. Teorías de la personalidad. , pp. 592.

CONDORI, H., 2012. *Un Modelo de Evaluación de Factores Críticos de Éxito en la Implementación de la Seguridad en Sistemas de Información para determinar su influencia en la intención del usuario*. S.l.: Universidad Inca Garcilaso de la Vega.

CONGRESO DE LA REPÚBLICA DEL PERÚ, 2011. Ley de protección de datos personales LEY Nº 29733. *Sistema Peruano de Información Jurídica* [en línea], pp. 1-17. Disponible en: http://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf.

CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA, 2016. PAe - MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [en línea]. [Consulta: 14 junio 2016]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WD9N8LIrJdg.

CONSUEGRA ANAYA, N., 2010. *Diccionario de Psicología*. 2a. ed. Bogotá: Ecoe Ediciones. ISBN 9789586486507.

CORTÉS, T., 2001. Una primera aplicacion de la teoria del comporta- miento planificado para explicar el abandono deltra- tamiento por parte de los dependientes alcoholicos. , vol. 54, no. 3, pp. 389-405.

DIRECCIÓN GENERAL DE ESTUDIOS ECONÓMICOS EVALUACIÓN Y COMPETITIVIDAD TERRITORIAL DEL VICEMINISTERIO DE MYPE E INDUSTRIA, 2014. Las MIPYMES en cifras 2013. . Lima, Perú:

EY-PERÚ, 2015. Perspectivas sobre Gobierno , Riesgo y Cumplimiento Adelántese a los delitos cibernéticos. . S.l.:

FEIST, J., 2007. Teorías de la personalidad. *Teorías de la personalidad*. 6ta Ed. Madrid: McGraw-Hill, pp. 270-291.

GOBIERNO/PERÚ, 2012. PROYECTO DE REGLAMENTO DE LA LEY No 29733 LEY DE PROTECCIÓN DE DATOS PERSONALES. *El Peruano* [en línea]. Lima, 2012. pp. 24. Disponible en: http://www.minjus.gob.pe/wp-content/uploads/2012/09/PROYECTO-REGLAMENTO-LEY-29733.pdf.

HAWKINS, J.D. y WEIS, J.G., 1995. El modelo del desarrollo social: un enfoque integrado a la prevención de la delincuencia. *Comunicación, Lenguaje y Educación*, vol. 7, pp. 115-133. ISSN 02147033. DOI 10.1174/021470395321341104.

HIRSCHI, T., 2003. Una teoría del control de la delincuencia. *Capítulo Criminológico*, vol. 31, no. 4, pp. 5-31.

INDECOPI, 2014. NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. *Norma Técnica Peruana* [en línea]. Lima, Perú: Disponible en: http://www.pecert.gob.pe/_publicaciones/2014/ISO-IEC-27001-2014.pdf.

INEI, 2009. Perú: Tecnologías de Información y Comunicaciones en las Empresas 2006-2007. . Lima, Perú:

INEI, 2015. Perú: Tecnologías de Información y Comunicación en las Empresas, 2015. . Lima, Perú:

ISO27000.ES, 2016. ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. .

LEE, S.M., LEE, S.G. y YOO, S., 2004. An integrative model of computer abuse based on social control and general deterrence theories. *Information and Management*, vol. 41, no. 6, pp. 707-718. ISSN 03787206. DOI 10.1016/j.im.2003.08.008.

LÓPEZ, R., 2014. Término C RIMIPEDIA : Teorías del control social. ,

MARTÍN, M.J., MANUEL, J. y ROJAS, D., 2011. Teoría del comportamiento planificado y conducta sexual de riesgo en hombres homosexuales. *. Rev Panam Salud Publica.*, vol. 29, no. 6, pp. 433-443. ISSN 10204989. DOI 10.1590/S1020-49892011000600009.

MINTIC, 2015. Seguridad de la Información. [en línea]. Bogota: Disponible en: http://www.digiware.net/sites/default/files/terpel.pdf.

MORENO MURCIA, J.A. y MARTÍNEZ CAMACHO, A., 2006. Importancia de la teoría de la autodeterminación en la práctica físico-deportiva: fundamentos e implicaciones prácticas. *Cuadernos de Psicoogia del Deporte*, vol. 6, no. 2, pp. 39-54.

ÖĞÜTÇÜ, G., TESTIK, Ö.M. y CHOUSEINOGLOU, O., 2016. Analysis of personal information security behavior and awareness. *Computers & Security* [en línea], vol. 56, pp. 83-93. ISSN 01674048. DOI 10.1016/j.cose.2015.10.002. Disponible en: http://www.sciencedirect.com/science/article/pii/S0167404815001406.

PONEMON INSTITUTE/LLC, 2016. 2016 Cost of Insider Threats Benchmark Study of Organizations in the United States Sponsored by Dtex. . S.l.:

PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA, 2013. *Gestión de riesgos* [en línea]. 2013. Bogotá Colombia: s.n. Disponible en: http://wsp.presidencia.gov.co/dapre/sigepre/Documents/Novedades/DAPRE-Gestion-riesgos-SIGEPRE2013.pdf.

REYES, M., 2011. *Propuestas para impulsar la seguridad informática en materia de educación*. S.l.: Universidad Nacional Autónoma de México.

ROBBINS, S.P., JUDGE, T.A., H, J.M.J. y ESTRADA, R.G., 2013. *Comportamiento-Organizacional-13a-Ed-_Nodrm*. 15. México, D.F.: Pearson Educación. ISBN 9786074420982.

ROJAS RODRÍGUEZ, C.A. y AGUILAR MARÍN, P., 2013. Metodología sistémica-cibernética para elaborar estructuras organizacionales dinámicas: aplicación a empresa de distribución de agua potable. *Revista CIENCIA Y TECNOLOGÍA* [en línea], vol. 9, no. 2, pp. 95-110. Disponible en: http://www.revistas.unitru.edu.pe/index.php/PGM/article/view/273/274.

SAFA, N.S., SOLMS, R. Von y FUTCHER, L., 2016. Human aspects of information security in organisations. *Computer Fraud and Security* [en línea], vol. 2016, no. 2, pp. 15-18. ISSN 13613723. DOI 10.1016/S1361-3723(16)30017-3. Disponible en: http://dx.doi.org/10.1016/S1361-3723(16)30017-3.

SAFA, N.S. y VON SOLMS, R., 2016. An information security knowledge sharing model in organizations. *Computers in Human Behavior* [en línea], vol. 57, pp. 442-451. ISSN 07475632. DOI 10.1016/j.chb.2015.12.037. Disponible en: http://dx.doi.org/10.1016/j.chb.2015.12.037.

SEALPATH, 2015. El eslabón más débil de la cadena de protección. [en línea]. [Consulta: 17 abril 2016]. Disponible en: http://www.sealpath.com/es/nosotros/blog/item/287-eslabon.

SOHRABI SAFA, N., VON SOLMS, R. y FURNELL, S., 2016. Information security policy compliance model in organizations. *Computers and Security* [en línea], vol. 56, pp. 1-13. ISSN 01674048. DOI 10.1016/j.cose.2015.10.006. Disponible en: http://dx.doi.org/10.1016/j.cose.2015.10.006.

SPITZNER, L., 2016. Securing the Human to be Mightier than the Computer. *Infosecurity* [en línea]. [Consulta: 11 agosto 2016]. Disponible en: https://www.infosecurity-

magazine.com/magazine-features/securing-the-human-mightier/.

SYMANTEC, 2014. Tendencias de Seguridad Cibernética en América Latina y el Caribe. . Washington D.C.:

TALAVERA ÁLVAREZ, V.R., 2013. *Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013*. S.l.: Pontificia Universidad Católica del Perú.

TELLEZ, J., 2008. *Derecho Informático*. México City: McGraw-Hill.

THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2013. DRAFT INTERNATIONAL STANDARD ISO / IEC FDIS Information technology — Security techniques — Code of practice for information security controls. , vol. 2013.

THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2016. Glosario de Iso/Iec 27000:2016. *ISO.org [Online]*, vol. 2016, pp. 38.

VILLENA AGUILAR, M.A., 2010. *Sistema de gestión de seguridad de información para una institución financiera* [en línea]. S.l.: PONTIFICIA UNIVERSIDAD CATOLICA DEL PERÚ. [Consulta: 12 septiembre 2016]. Disponible en: http://tesis.pucp.edu.pe:8080/repositorio/bitstream/handle/123456789/362/VILLENA_MOISÉS_SISTEMA_DE GESTIÓN_DE_SEGURIDAD_DE_INFORMACIÓN_PARA_UNA_INSTITUCIÓN_FINANCIERA.pdf?sequence=1&isAllowed=y.

ANEXOS

1. ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.

5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.

6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la seguir de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.

6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.

7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la informac.
7.2.3 Proceso disciplinario.

7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.

8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.

8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.

8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.

9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.

9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso

9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.

9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.

10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.

11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.

11.1.6 Áreas de acceso público, carga y descarga.

11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.

12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.

12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.

12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.

12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.

12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.

12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.

12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.

13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.

13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.

14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.

14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.

15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
Cadena de suministro en tecnologías de la información y comunicaciones.

15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.

ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

17.2 Redundancias.
Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.

18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.

18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento

2. Encuesta para Sub Gerente de TI

Encuesta sobre temas de seguridad de la información para el ACPNA - Región Centro - 2017

La siguiente encuesta tiene como propósito recopilar información sobre la seguridad de la información dentro del ACPNA. Dicha información será utilizada como parte de un estudio para la obtención de un grado universitario y para ayudar a fortalecer la seguridad de la información dentro de la institución. Toda información recopilada se mantendrá en completa discreción y no se utilizará para otros fines.

	Pregunta	Respuesta
	Seguridad de la Información	
1	¿Existe un área de seguridad de la información en la empresa?	
2	¿Existe alguna política o normativa de seguridad de la información en la institución?	
3	¿Se considera la seguridad de la información en proyectos de cualquier índole emprendidos por la institución?	
4	¿Existe alguna persona designada oficialmente que pueda resolver sus dudas con respecto a la seguridad de la información?	
5	¿Tienen su árbol normativo completo? ¿Políticas, normas, procedimientos e instructivos?	
6	¿Tiene una gestión de RFC establecida?	
7	¿Tienen un inventario de activos actualizados (Incluidas personas clave)?	
8	¿Tienen propietarios para los activos de información?	
9	¿Se tienen una clasificación y valoración de los activos de información?	
10	¿Se tienen identificadas las vulnerabilidades de los activos de información?	
11	¿Se ha realizado un análisis de riesgos de seguridad de la información?	

12	¿Se tienen implementados controles para los riesgos encontrados?	
13	¿Cree usted que es necesario implementar algún tipo de protección de la información para la institución?	
14	¿Existen políticas, normas y procedimientos de gestión de accesos a sus sistemas?	
15	¿Se realiza una verificación de accesos y privilegios periódicamente?	
16	¿Se cuentan con indicadores de cumplimiento de políticas, planes y procedimientos de seguridad de la información?	
17	¿Se verifica el Currículum Vitae de personal relacionada al tratamiento de información confidencial y datos personales de la empresa?	
18	¿Se verifica si personal relacionado a la seguridad perimetral tiene antecedentes penales?	
19	¿Se verifica si personal relacionado a la seguridad lógica de la información tiene antecedentes penales?	
20	¿Existe una clausula en los contratos que se refieran a la información que se pone a disposición del contratado?	
21	¿Dentro de la descripción de sus roles y funciones, se encuentra algún tipo de guía que contenga las expectativas, guías, necesidad de estudio o similares de cómo mantener la seguridad de la información que manejan?	
22	¿Existe algún tipo de sanción establecida para algún empleado que de manera voluntaria o involuntaria afecte la integridad, confidencialidad y disponibilidad de la información en la institución?	
23	¿En sus contratos con terceros se consideraron adendas de seguridad específicas y alineadas a la protección de información y datos personales de la institución?	
24	¿Tienen y manejan un documento de confidencialidad de datos según su cargo?	
25	¿Tienen un procedimiento de cese de usuarios?	
26	¿Realizan pruebas de ingeniería social?	
27	¿Existe una política, procedimiento o guía de mantenimiento de equipos?	

28	¿Existe un registro o bitácora de fallas detectas en el sistema y como se solucionaron dichas fallas?	
29	¿Realizan actualización de antivirus en las computadoras de sus usuarios?	
30	¿Realizan actualización de software periódicamente?	
31	¿Realizan actualización de los sistemas operativos?	
32	¿Aplican criptografía a datos confidenciales y personales y contraseñas como AES 256, contraseñas hash 256?	
33	¿Aplican criptografía a transmisión de datos entre sedes?	
34	¿Tienen restricciones en el acceso de computadoras en sitios públicos?	
35	¿Utilizan algún tipo de hardware de seguridad como IPS, firewall, WSG (Filtro Web), UTM, NAC (Network Access Center), SEG (Secure Email Gateway), etc.?	
36	¿Utilizan una configuración de Firewall definida en sus servidores?	
37	¿Tienen reglas de firewall definidas y establecidas?	
38	¿Utilizan un procedimiento de directorio activo en sus ordenadores?	
39	¿Cuentan con log, y pistas de auditoría en sus sistemas?	
40	¿Han tenido alguna auditoría de seguridad de la información?	
41	¿Ha realizado pruebas de penetración de sistemas?	
42	¿Han realizado hacking ético alguna vez?	
43	En contrato de servicios como internet, ¿Tienen cláusulas de SLA establecidas y orientadas a su seguridad de la Información?	
44	¿Tienen una Configuración de BD personalizada y orientada a la seguridad de la información evitando los súper usuarios?	

45	¿Tienen diversos tipos de usuarios de acceso a las bases de datos?	
46	¿Tienen los datos sensibles encriptados en su base de datos?	
47	¿Tienen políticas, procedimientos e instructivos de backup?	
48	¿Realizan pruebas de integridad de los datos periódicamente?	
49	¿Aplican segregación de funciones en su manejo de base de datos?	
50	¿Tienen sus requerimientos de seguridad identificados?	
51	¿Utilizan Distribución de la red por medio de Vlans definidas?	
52	¿Utilizan encriptación en los equipos donde tienen información confidencial como en las computadoras de gerencia o áreas de contabilidad?	
53	¿Se tienen logs de verificaciones de seguridad en supervisiones periódicas?	
54	¿Existe una restricción de instalación de software?	
55	¿Tienen una política de cambio de contraseñas periódicamente para el área de TI?	
56	¿Tienen una política de cambio de contraseñas periódicamente para los usuarios de sus sistemas?	
57	¿Existe un manual de uso de equipo informático que informa de lo que se debe y no debe hacer con tal equipo?	
58	¿Se considera el ciclo de vida de la información que se maneja en la institución en el manejo de dicha información?	
59	¿Realizan una supervisión de la red, equipos y dispositivos de la institución?	
60	¿Tienen aplicaciones bloqueadas para sus diversos usuarios?	
61	¿Existe un programa de capacitaciones en temas de seguridad de la información?	

62	¿Existe algún medio alternativo donde se reciba actualizaciones sobre seguridad de la información?	
63	¿Se brinda capacitación sobre protección de datos personales?	
64	¿Se brinda capacitación sobre Ingeniería social en la institución?	
65	¿Se brinda capacitación sobre el uso de contraseñas seguras?	
66	¿Se brinda capacitación sobre Gestión de archivos confidenciales y como tratarlos?	
67	¿Se brinda capacitación sobre ataques de virus informáticos y su propagación?	
68	¿Se brinda capacitación sobre riesgos de seguridad de la información?	
69	¿Existe alguna política de actualizaciones a las computadoras de usuarios?	
70	¿Se realizan actualizaciones periódicas de SO a las computadoras de sus usuarios?	
71	¿Sigue Usted un proceso específico para la información que maneja dentro del ciclo de vida de la información?	
72	¿Se tiene un registro de personal autorizado para ciertas áreas de la institución?	
73	¿Se tiene un registro de incidentes y medidas adoptadas relacionadas a la seguridad de la información?	
74	¿Se menciona en su contrato alguna disposición con respecto a la confidencialidad y protección de datos personales e información de la empresa?	
75	¿Se revisan los logs de acceso periódicamente?	
76	¿Se realizan cambios de contraseña a roles de administración en servidores, switches, bases de datos, etc.? ¿Cada que tiempo?	
77	¿Existe un log de accesos satisfactorios y denegados?	
78	¿Sus sistemas cierran las sesiones si se detecta inactividad luego de un tiempo determinado?	

79	¿Cierra sus sesiones de usuario cuando no los utiliza o se ausenta, así se por un instante?	
80	¿Se cuenta con procedimientos de Roll-back o regreso a versiones previas en sus sistemas?	
81	¿Su área de desarrollo de software utiliza diferentes dominios y directorios que sus sistemas en operación?	
82	¿Se cuenta con protección antimalware en la institución para cada terminal?	
83	¿Se tienen políticas de recuperación ante ataques de malware?	
84	¿Se tiene un plan de continuidad de negocio para la institución?	
85	¿Se tiene un plan de continuidad de seguridad de la información para la institución?	
	Software	
86	¿Utilizan estándares de seguridad en el desarrollo de software como SAMM, ISO 27034, SD3?	
87	¿Aplican segregación de funciones en su programación de aplicaciones?	
88	¿Ha realizado una revisión de código de sistemas en fase de producción?	
89	¿Se consideran bloqueos para sistemas luego de un número de intentos fallidos de ingreso de contraseña?	
90	¿Se utiliza algún sistema de re-CAPTCHA en sus sistemas?	
91	En el área de desarrollo, ¿Almacenan el código en desarrollo en un lugar seguro?	
92	En el proceso de desarrollo de software ¿Se realizan pruebas de funcionalidad de seguridad?	
93	¿Se utilizan procedimientos almacenados en la base de datos antes de programar?	
94	Antes de que un sistema pase a producción, ¿Se realizan pruebas de aceptación y seguridad?	

	Data center	
95	¿Su data center cuenta con seguridad de acceso físico?	
96	¿Su data center cuenta con seguridad de ventilación adecuada?	
97	¿Su data center cuenta con gestión de accesos?	
98	¿Su data center cuenta con cámaras de vigilancia?	
99	¿Su data center cuenta con cableado eléctrico aislado?	
100	¿Su data center cuenta con cableado de datos estructurado?	
101	¿Su data center cuenta con sistema contra incendio?	
102	¿Su data center cuenta con falso piso?	
103	¿Su data center cuenta con gabinetes asegurados?	
104	¿Tiene sólo los puertos de servidores que utilizan mientras los demás están cerrados?	
105	¿Realizan actualización de parches de seguridad en sus servidores?	
106	¿Realizan actualización de SO en sus servidores?	
	Ley de datos personales	
107	¿Conoce usted sobre el alcance de la Ley 29733?	
108	¿Conoce el tipo de empresa y nivel que esta tiene según la directiva de seguridad de la Ley 29733?	
109	¿Conoce los requerimientos de seguridad que exige la ley sobre la protección de datos personales?	

110	¿Existe una política de protección de datos personales?	
111	¿Su área ha implementado los requisitos de seguridad que exige la ley sobre la protección de datos personales?	
112	¿Tiene su banco de datos registrado ante la autoridad nacional de datos personales?	
113	¿Se considera en sus contratos con terceros el manejo de datos personales según la ley 29733?	
114	¿Existe un documento de información y consentimiento de uso de datos personales disponible para los usuarios cuya información se registra en sus sistemas?	
115	¿Los usuarios, cuyos datos ustedes tienen, fueron informados sobre el uso de sus datos de forma previa, informada, expresa e inequívoca según el artículo 18 de la ley 29733?	
116	¿Tienen algún tratamiento especial para datos sensibles según dispone la ley 29733?	
117	¿Tiene algún tratamiento especial para información de menores de edad?	
118	¿Se realiza un estudio de antecedentes a personal que tiene acceso a información confidencial o de carácter privado?	
	Preguntas abiertas	
119	¿Qué criterios siguen para elegir la tecnología que utilizan en su área?	
120	¿Qué consideraciones mínimas tienen para la adquisición y compra de Hardware y software?	
121	¿Cómo ha influenciado su área a las otras áreas de la empresa en los últimos años?	
122	¿Qué planes de seguridad de la información tiene su área?	
123	¿Qué planes tiene su área sobre el cumplimiento de la ley 29733?	

3. Encuesta para Sub Gerente de Recursos Humanos

Encuesta sobre temas de seguridad de la información para el ACPNA - Región Centro - 2017

La siguiente encuesta tiene como propósito recopilar información sobre la seguridad de la información dentro del ACPNA. Dicha información será utilizada como parte de un estudio para la obtención de un grado universitario y para ayudar a fortalecer la seguridad de la información dentro de la institución. Toda información recopilada se mantendrá en completa discreción y no se utilizará para otros fines.

	Pregunta	Respuesta
1	¿Tienen un procedimiento documentado de cese de usuarios?	
2	¿Se realiza un estudio de antecedentes penales a personal que tiene acceso a información confidencial o de carácter privado?	
3	¿Se verifica el Currículum Vitae de personal relacionada al tratamiento de información confidencial y datos personales de la empresa?	
4	¿Se verifica si personal relacionado a la seguridad perimetral tiene antecedentes penales?	
5	¿Se verifica si personal relacionado a la seguridad lógica de la información tiene antecedentes penales?	
6	¿Existe una clausula en los contratos que se refieran a la información que se pone a disposición del contratado?	
7	¿Dentro de la descripción de sus roles y funciones, se encuentra algún tipo de guía que contenga las expectativas, guías, necesidad de estudio o similares de cómo mantener la seguridad de la información que manejan?	
8	¿Existe algún tipo de sanción para algún empleado que de manera voluntaria o involuntaria afecte la integridad, confidencialidad y disponibilidad de la información en la institución?	
9	¿Coordina su área algún tipo de capacitación con respecto a la seguridad de la información?	
10	¿Tienen y manejan un documento de confidencialidad de datos según su cargo?	
11	¿Se tiene un registro de personal autorizado para ciertas áreas de la institución?	
12	¿Se realizado alguna vez una encuesta de satisfacción laboral?	

4. Encuesta para personal de la institución

	Encuesta sobre temas de seguridad de la información para el ACPNA - Región Centro - 2017				
	La siguiente encuesta tiene como propósito recopilar información sobre la seguridad de la información dentro del ACPNA. Dicha información será utilizada como parte de un estudio para la obtención de un grado universitario y para ayudar a fortalecer la seguridad de la información dentro de la institución. Toda información recopilada se mantendrá en completa discreción y no se utilizará para otros fines.				
	Pregunta	**Persona 1**	**Alternativas**		
	Plan de gestión de seguridad de la información				
1	¿Tiene la institución algún plan para proteger la información dentro de ella?		**Si**	**No**	**No aplica**
2	¿Cree usted que es necesario implementar algún tipo de protección de la información para la institución?		**Si**	**No**	**No aplica**
3	¿Estaría dispuesto a apoyar activamente a la implementación de algún proyecto de seguridad de la información?		**Si**	**No**	**No aplica**
	Dirección del área de seguridad de la información				
4	¿Existe un área de seguridad de la información en la institución?		**Si**	**No**	**No aplica**
5	¿Existe alguna persona designada oficialmente que pueda resolver sus dudas con respecto a la seguridad de la información?		**Si**	**No**	**No aplica**
	Políticas, normas, procedimientos e instructivos en procesos de información clave de la empresa				
6	¿Tiene la institución políticas, normas y procedimientos de seguridad de la información establecidas y documentadas?		**Si**	**No**	**No aplica**
7	¿Tiene la empresa una política de control de accesos para diversos usuarios y roles?		**Si**	**No**	**No aplica**
8	¿Se tienen los procesos de manejo de información documentados?		**Si**	**No**	**No aplica**
9	¿Se considera el ciclo de vida de la información en la información que se maneja en la institución?		**Si**	**No**	**No aplica**
10	¿Existe un manual de uso de equipo informático que le informa de lo que debe y no debe hacer con tal equipo?		**Si**	**No**	**No aplica**
11	¿Existe una restricción de instalación de software en su computadora?		**Si**	**No**	**No aplica**

12	¿Tienen sitios web bloqueados en sus equipos de cómputo por parte de TI?		**Si**	**No**	**No aplica**
13	¿Tienen aplicaciones bloqueadas en sus equipos de cómputo por parte de TI?		**Si**	**No**	**No aplica**
14	¿La institución, tiene una política de cambio periódico de contraseñas?		**Si**	**No**	**No aplica**
15	¿Cómo parte de las políticas de seguridad, es usted forzado a cambiar sus contraseñas periódicamente?		**Si**	**No**	**No aplica**
16	¿Le permiten cambiar sus contraseñas de acceso cuando usted lo considera necesario en los sistemas de la institución?		**Si**	**No**	**No aplica**
	Programa de gestión de incidentes de seguridad de la información				
17	¿Se tiene un registro de incidentes y medidas adoptadas relacionadas a la seguridad de la información?		**Si**	**No**	**No aplica**
18	¿Sabe a quién reportar una sospecha o incidente de seguridad de la información?		**Si**	**No**	**No aplica**
19	¿Ha reportado incidentes relacionados a acceso no autorizado de personas?		**Si**	**No**	**No aplica**
	Capacitaciones sobre seguridad de la información hasta la fecha				
20	¿Recibe usted información sobre riesgos de seguridad de la información de parte del área competente?		**Si**	**No**	**No aplica**
21	¿Existe un programa de capacitaciones en temas de seguridad de la información?		**Si**	**No**	**No aplica**
22	¿Se brinda capacitación sobre protección de datos personales?		**Si**	**No**	**No aplica**
23	¿Se brinda capacitación sobre Ingeniería social en la institución?		**Si**	**No**	**No aplica**
24	¿Se brinda capacitación sobre el uso de contraseñas seguras?		**Si**	**No**	**No aplica**
25	¿Se brinda capacitación sobre Gestión de archivos confidenciales y como tratarlos?		**Si**	**No**	**No aplica**
26	¿Se brinda capacitación sobre ataques de virus informáticos y su propagación?		**Si**	**No**	**No aplica**

27	¿Se brinda capacitación sobre riesgos de seguridad de la información?		**Si**	**No**	**No aplica**		
28	¿Existe algún medio alternativo donde reciba actualizaciones sobre seguridad de la información?		**Si**	**No**	**No aplica**		
	Hábitos de seguridad de la información						
29	¿Cuánto de los hábitos de seguridad de la información conoce y aplica?		**Nada**	**Sólo unos pocos hábitos**	**En lo personal**	**En lo personal y algo en lo laboral**	**Siempre en cada aspecto de mi vida**
30	¿Sigue Usted un proceso específico para la información que maneja dentro del ciclo de vida de la información?		**Si**	**No**	**No aplica**		
31	¿Cierra sus sesiones de usuario cuando no las utiliza o se ausenta, así sea por un instante?		**Si**	**No**	**No aplica**		
32	¿Comparte sus cuentas de usuario y contraseñas con otros colegas?		**Si**	**No**	**No aplica**		
33	¿Cambia usted sus contraseñas de los sistemas de la institución periódicamente?		**Si**	**No**	**No aplica**		
34	¿Cada cuánto cambia sus contraseñas?		**Si**	**No**	**No aplica**		
35	¿Abre archivos adjuntos en correos de personas ajenas a la institución?		**Si**	**No**	**No aplica**		
36	¿Accede a sitios web no confiables dentro del lugar de trabajo?		**Si**	**No**	**No aplica**		
37	¿Utiliza sitios de redes sociales durante horario de trabajo?		**Si**	**No**	**No aplica**		
38	¿Abre enlaces dentro de correos de personas ajenas a la institución?		**Si**	**No**	**No aplica**		
39	¿Utiliza acceso a internet de lugares públicos para acceder a sus cuentas de correo e información de la empresa?		**Si**	**No**	**No aplica**		
40	¿Ha conectado algún dispositivo extraíble o móvil personal en su computadora de trabajo?		**Si**	**No**	**No aplica**		
41	¿Alguna vez ha insertado un dispositivo extraíble en su computadora que le obsequiaron o que encontró?		**Si**	**No**	**No aplica**		
42	¿Utiliza medios móviles para el manejo de correo institucional?		**Si**	**No**	**No aplica**		

43	¿Utiliza solo software autorizado por la empresa?		**Si**	**No**	**No aplica**		
44	¿Destruye y se deshace apropiadamente de documentos que contienen información sensible?		**Si**	**No**	**No aplica**		
45	¿Deja documentación que contiene información confidencial sobre su escritorio de trabajo durante la noche?		**Si**	**No**	**No aplica**		
46	¿Se encuentra vigilante para reconocer y acercarse a personas no autorizadas en lugares confidenciales?		**Si**	**No**	**No aplica**		
	Conocimiento de seguridad de la información						
47	¿La institución le anima a adquirir conocimiento y habilidades sobre temas de seguridad de la información?		**Si**	**No**	**No aplica**		
48	¿Dentro de la descripción de sus roles y funciones, se encuentra algún tipo de guía que contenga las expectativas, procedimientos, necesidad de estudio o similares de cómo mantener la seguridad de la información que manejan?		**Si**	**No**	**No aplica**		
51	¿Comparte conocimiento de seguridad de la información con sus colegas?		**Si**	**No**	**No aplica**		
49	¿Cuánto conoce sobre temas de Seguridad de la información?		**Nada**	**Poco**	**Lo básico**	**Conocimiento intermedio**	**Conocimiento Avanzado**
50	¿Cuánto conoce usted sobre la ley de protección de datos personales?		**Nada**	**Poco**	**Lo básico**	**Conocimiento intermedio**	**Conocimiento Avanzado**
	Confidencialidad de información en la empresa						
			Si	**No**	**Blanco**		
52	Cuándo asumió su puesto, ¿Se le brindó algún tipo de inducción en referencia al tratamiento de la información de la cual hace uso?		**Si**	**No**	**No aplica**		
53	¿Se menciona en su contrato alguna disposición con respecto a la confidencialidad y protección de datos personales e información de la empresa?		**Si**	**No**	**No aplica**		
54	¿Existe una clausula en los contratos que se refiera qué información se pone a disposición del contratado?		**Si**	**No**	**No aplica**		
55	¿Los usuarios, cuyos datos ustedes tienen, fueron informados sobre el uso de sus datos de forma previa, informada, expresa e inequívoca según el artículo 18 de la ley 29733 sobre tratamiento de datos personales?		**Si**	**No**	**No aplica**		

56	¿Sabe si existe un documento de información y consentimiento de uso de datos personales disponible para los usuarios cuya información se registra en sus sistemas?		**Si**	**No**	**No aplica**		
57	¿Tiene algún tratamiento especial para datos personales de menores de edad?		**Si**	**No**	**No aplica**		
58	En su área, ¿Utilizan encriptación de datos con respecto a información sensible o confidencial para la institución?		**Si**	**No**	**No aplica**		
	Satisfacción laboral en la empresa						
59	De forma confidencial, ¿Se encuentra satisfecho con la labor que le asignaron dentro de la institución?		**No satisfecho**	**Poco Satisfecho**	**Algo Satisfecho**	**Satisfecho**	**Muy satisfecho**
60	De forma confidencial, ¿Se encuentra satisfecho con su actual puesto y los beneficios que recibe de la institución?		**No satisfecho**	**Poco Satisfecho**	**Algo Satisfecho**	**Satisfecho**	**Muy satisfecho**

5. Resultados de encuestas y porcentajes permitidos de publicar

Encuesta sobre temas de seguridad de la información para el ACPNA - Región Centro - 2018					
La siguiente encuesta tiene como propósito recopilar información sobre la seguridad de la información dentro del ACPNA. Dicha información será utilizada como parte de un estudio para la obtención de un grado universitario y para ayudar a fortalecer la seguridad de la información dentro de la institución. Toda información recopilada se mantendrá en completa discreción y no se utilizará para otros fines.					
Pregunta	**Sí**	**No**	**Blanco**	**Porcentaje de Sí**	**Porcentaje de No**
Plan de gestión de seguridad de la información					
¿Tiene la institución algún plan para proteger la información dentro de ella?	2	33	0	6	94
¿Cree usted que es necesario implementar algún tipo de protección de la información para la institución?	35	0	0	100	0
¿Estaría dispuesto a apoyar activamente a la implementación de algún proyecto de seguridad de la información?	35	0	0	100	0
Dirección del área de seguridad de la información				0	
¿Existe un área de seguridad de la información en la institución?	0	35	0	0	100
¿Existe alguna persona designada oficialmente que pueda resolver sus dudas con respecto a la seguridad de la información?	6	29	0	17	83
Políticas, normas, procedimientos e instructivos en procesos de información clave de la empresa					0
¿Tiene la institución políticas, normas y procedimientos de seguridad de la información establecidas y documentadas?	4	31	0	11	89
¿Existe una restricción de instalación de software en su computadora?	29	6	0	83	17
¿Tienen aplicaciones bloqueadas en sus equipos de cómputo por parte de TI?	16	19	0	46	54
Programa de gestión de incidentes de seguridad de la información				0	0
¿Se tiene un registro de incidentes y medidas adoptadas relacionadas a la seguridad de la información?	2	33	0	6	94
¿Ha reportado incidentes relacionados a acceso no autorizado de personas?	10	25	0	29	71
Capacitaciones sobre seguridad de la información hasta la fecha				0	0

¿Existe un programa de capacitaciones en temas de seguridad de la información?	0	35	0	0	100
Hábitos de seguridad de la información					
	Nada	**Sólo unos pocos hábitos**	**En lo personal**	**En lo personal y algo en lo laboral**	**Siempre en cada aspecto de mi vida**
¿Cuánto de los hábitos de seguridad de la información conoce y aplica?	12	20	2	1	0
	Si	**No**	**Blanco**		
Conocimiento de seguridad de la información					
	Nada	**Poco**	**Lo básico**	**Conocimiento intermedio**	**Conocimiento Avanzado**
¿Cuánto conoce sobre temas de Seguridad de la información?	20	12	2	1	0
Confidencialidad de información en la empresa					
	Si	**No**	**Blanco**		
¿Se menciona en su contrato alguna disposición con respecto a la confidencialidad y protección de datos personales e información de la empresa?	15	20	0	43	57
¿Existe una clausula en los contratos que se refiera qué información se pone a disposición del contratado?	5	30	0	14	86
Satisfacción laboral en la empresa					
	No satisfecho	**Poco Satisfecho**	**Algo Satisfecho**	**Satisfecho**	**Muy satisfecho**
De forma confidencial, ¿Se encuentra satisfecho con su actual puesto y los beneficios que recibe de la institución?	30	1	0	3	1

6. Formato de análisis de activos de la información

Código de activo	Nombre del Activo	Descripción del activo	Área de la empresa que lo utiliza	¿Donde se almacena?	Tangible o intangible	Clasificacion			Clasificación final (Importancia del activo)	Custodio del activo
						Criticidad	Frecuencia de uso	Tecnologia		

7. Matriz de riesgos y de controles

Descripción del riesgo								Evaluación de riesgo			
Código de activo	Nombre del Activo	Vulnerabilidad	Amenaza	Código de riesgo	Riesgo (Detallar)	¿Qué origina el riesgo?	Consecuencia del riesgo	Probabilidad de ocurrencia (Valores entre 1 y 5)	Impacto sobre el activo (Valores entre 1 y 5)	Valor del riesgo	Estrategia de respuesta al riesgo
Act001	Examen de clasificación	Falta de mecanismos de monitoreo	Robode infomración	Ri001	Sustracción del examen de clasificación	Profesores	El examen puede ser robado y difundido y puede perder confiabilidad	3	4	12	Mitigar
		Ausencia de personal	Robo de información	Ri002	Sustracción de los examenes de clasificación en ausencia del personal	Profesores	El examen puede ser robado y difundido y puede perder confiabilidad	3	4	12	Mitigar

8. Cuadro de indicadores de evaluación del modelo

Indicadores de evaluación para el modelo			
Se recomienda realizar la evaluación del modelo a un año de su implementación luego de que este consolidado el modelo en la empresa y se hagan revisiones constantes y evaluaciones a la implementación del mismo. Del mismo modo, se debe evaluar la efectividad de la gestión de seguridad de la información en la empresa periódicamente considerando los criterios mencionados.			
Indicador	**Descripción**	**Antes de implementación del modelo**	**Primera evaluación**
Plan de gestión de seguridad de la información	Este indicador evalúa si es que estableció o no un plan de seguridad de la información que da inicio a la gestión de seguridad de la información. O%= no realizado; 100%= realizado.	Inexistente, 0%	
Implementación del modelo de seguridad	Este indicador considera el porcentaje de implementación del modelo de seguridad de la información dentro de la empresa. De 0 a 100%.	No realizado, 0%	
Identificación de activos críticos	Este indicador permite identificar si se ha realizado un inventario de activos de seguridad de la información dentro de la empresa. O%= no realizado; 100%= realizado.	Nunca realizado, 0%	
Identificación de vulnerabilidades y riesgos	Matriz de riesgos de los activos de información.	Nunca realizado, 0%	
Implementación de controles	Implementación de controles identificados en los activos de información. Núm. de controles / Núm.. Activos * 100	Inexistente, 0%	
Número de personas asignadas a la gestión de seguridad de la información	Gestor de la seguridad de la información designado en la empresa. Sin gestor = 0%; con gestor= 100%	Ninguna, 0%	
Comité de seguridad de la información	Formación y conformación del comité de seguridad de la información dentro de la empresa. Sin comité = 0%; Con comité = 100%.	Inexistente, 0%	
Programa de gestión de incidentes de seguridad de la información	Contempla la implementación de la gestión de incidentes de seguridad de la información en la empresa. O%= no realizado; 100%= realizado.	Inexistente, 0%	
Existencia de políticas, normas, procedimientos e instructivos en procesos de información clave de la empresa	Considera la existencia de políticas, normas, procedimientos e instructivos de seguridad de la información en procesos clave de la empresa. O%= no realizado; 100%= realizado.	Inexistente, 0%	
Numero de auditorías realizadas (Mínimo 1)	Número de auditorías de seguridad de la información realizadas en la empresa. Mínimo 1 anual. O%= no realizado; 100%= realizado.	Ninguna, 0%	
Número de capacitaciones sobre seguridad de la información hasta la fecha	Se refiere a la cantidad de capacitaciones de seguridad de la información realizadas en un periodo determinado.	Ninguna, 0%	

Promedio de calificaciones de evaluaciones sobre conocimiento de seguridad de la información	Es el promedio de calificaciones obtenidas en las evaluaciones de los trabajadores con respecto a la seguridad de la información.	Nunca realizado, 0%	
Tratamiento del personal para identificar comportamientos de riesgo en Seguridad de la Información	Estudio realizado como parte del modelo de gestión de seguridad de la información para identificar, por medio de un estudio psicológico, posibles comportamientos de riesgo de los trabajadores en la empresa. O%= no realizado; 100%= realizado.	Nunca realizado, 0%	
Índice de satisfacción laboral en la empresa	Describe el resultado en porcentaje del estudio de satisfacción laboral realizado en la empresa.	Nunca identificado, 0%	