UNIVERSIDAD PRIVADA TELESUP

FACULTAD DE INGENIERÍA DE SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA Y ARQUITECTURA

TESIS

PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, APLICANDO LA METODOLOGÍA MAGERIT PARA EL GOBIERNO REGIONAL PUNO CASO: PROYECTO ESPECIAL CAMÉLIDOS SUDAMERICANOS – PECSA, 2017

PARA OBTENER EL TÍTULO DE:

INGENIERO DE SISTEMAS E INFORMÁTICA

AUTOR:

Bach. WILLIAM YANA VIVEROS

LIMA – PERÚ

2018

ASESOR DE TESIS

……..……..

Mg. DENIS CHRISTIAN OVALLE PAULINO

JURADO EXAMINADOR

……..……

Dr. ISSAAK RAFAEL VASQUEZ ROMERO

PRESIDENTE

……..……

Mg. EDMUNDO JOSE BARRANTES RIOS

SECRETARIO

……..……

Dra. MADELAINE BERNARDO SANTIAGO

VOCAL

DEDICATORIA

A mis padres Dionicio y Pascuala, por estar siempre presente en mi vida; y sé que están orgullosos de la persona en la cual me he convertido.

A todos ellos se los agradezco de todo corazón. Para todos ellos hago esta dedicatoria.

A mi esposa Yaneth, por su amor permanente, cariño y comprensión.

A mis maestros y amigos, quienes sin su ayuda nunca hubiese podido hacer esta tesis.

AGRADECIMIENTOS

A la Universidad Privada TELESUP, por darme la oportunidad de superarme en el aspecto profesional y como persona.

A mi asesor de investigación, por orientarme a seguir el camino de indagación de mi trabajo de investigación final.

Al Proyecto Especial Camélidos Sudamericanos - PECSA, por la oportunidad brindada al facilitarme el acceso a la información importante para realizar un trabajo sin igual.
Muchas gracias.

RESUMEN

El objetivo de la investigación es establecer un Sistema de Gestión de Seguridad de Información, aplicando la metodología Magerit para el Proyecto Especial Camélidos Sudamericanos – PECSA del Gobierno Regional de Puno, con el fin de proponer una política y manual de SGSI para proteger la información, y así brindar una adecuada atención con respecto a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, a los criadores de alpaca de la Región Puno.

La metodología usada para el análisis de riesgos es el MAGERIT, donde paso a paso se procede a inventariar los activos, la valoración cualitativa de los activos, identificación de salvaguardas para los activos, valoración y evaluación de riesgos y el informe de calificación del riesgo, que permitieron identificar los riesgos de la información del proyecto.

Los resultados del diagnóstico obtenidos mediante la Entrevista, determino que no se encuentra seguro la información y/o documentación técnica, financiera y administrativa que sustentan el cumplimiento de las actividades del PECSA; Se desarrollaron las etapas de la metodología de análisis de información, a través de la aplicación de una investigación de campo al personal que labora en el PECSA. Finalmente se resuelve, se realizó la propuesta de un Sistema de Gestión de Seguridad de Información para preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

Palabras claves:
Gestión de Seguridad, Seguridad de la información, Metodología MAGERIT.

ABSTRACT

The objective of the research is to establish an Information Security Management System, applying the Magerit methodology for the Special South American Camelids Project - PECSA of the Regional Government of Puno, in order to propose an ISMS policy and manual to protect the information, and thus provide adequate attention with respect to the confidentiality, integrity, availability, authenticity and traceability of the information, to the alpaca breeders of the Puno Region.

The methodology used for the risk analysis is the MAGERIT, where step by step we proceed to inventory the assets, the qualitative valuation of the assets, identification of safeguards for the assets, valuation and evaluation of risks and the risk rating report, that allowed to identify the risks of the project information.

The results of the diagnosis obtained through the Interview, determined that the information and / or technical, financial and administrative documentation supporting the fulfillment of PECSA activities is not secure; The stages of the information analysis methodology were developed, through the application of a field investigation to the personnel that works in the PECSA. Finally, it is resolved, the proposal of an Information Security Management System was made to preserve the confidentiality, integrity, availability, authenticity and traceability of the information.

Keywords:

Security Management, Information Security, MAGERIT Methodology.

INDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

En la actualidad se utiliza sistemas informáticos que sirven para almacenar, procesar y transmitir la información que se encuentra en toda clase de instituciones de diferentes rubros y funciones según Vasco Rodrigo.

De esta forma se entiende que existen una cantidad cada vez mayor de personas que tienen acceso a la información que podría ser crítica para las diferentes instituciones que trabajan. Por lo tanto, siempre se tiene presente el riesgo de fuga de información sensible, ya sea por medio de personas que cuentan con acceso a dicha información, o por terceras personas. El presente trabajo consta de 7 capítulos.

El capítulo I, hace referencia al problema de la investigación, el cual consiste en dar a conocer la descripción del problema, describir los problemas que llevaron a realizar el presente trabajo con los objetivos de la investigación.

El Capítulo II, presentan el Marco Teórico, donde se dará a conocer los antecedentes de la investigación, como nacionales e internacionales, así como también las bases teóricas de las variables y la definición de términos básicos.

El Capítulo III, describe el Marco Metodológico, que consiste en determinarla hipótesis, la variable de estudio, el tipo, nivel de investigación, población y la muestra seleccionada para el estudio de la investigación.

El Capítulo IV, se refiere a la Solución Tecnológica y la propuesta del Sistema de Gestión de Seguridad de la Información. En los capítulos V, VI y VII se refiere a la discusión, conclusión y las recomendaciones referentes al análisis e interpretación de los resultados, que se realizó a través de la entrevista. Para así demostrar la Hipótesis General que se ha planteado. El propósito es conseguir niveles adecuados de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de toda la información institucional relevante, con el fin de asegurar la continuidad operacional de los procesos y servicios, mediante un SGSI y que esperemos brinde los propósitos necesarios del tema.

I. PROBLEMA DE INVESTIGACIÓN

1.1. Planteamiento del Problema

En la actualidad, las empresas de cualquier tipo o sector de actividad se enfrentan cada vez más con riesgos e inseguridades procedentes de una amplia variedad de contingencias, las cuales pueden dañar considerablemente tanto los sistemas de información como la información procesada y almacenada según lo manifiesta Gómez Fernández y Andrés Álvarez, (2012). Un Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización. Su implantación supone el establecimiento de procesos formales y una clara definición de responsabilidades en base a una serie de políticas, planes y procedimientos que deberán constar como información documentada según lo manifiestan Gómez Fernández y Fernández Rivero, (2014).

En el Perú según la Norma Técnica Peruana el Sistema de Gestión de la Seguridad de la Información preserva la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos y proporciona confianza a las partes interesadas en el sentido en que los riesgos se manejan adecuadamente. Es importante que el Sistema de Gestión de la Seguridad de la Información sea parte y esté integrado con los procesos de la organización y la estructura de gestión general y que la seguridad de la información se considere en el diseño de procesos, sistemas y controles de la información. Se espera que la Implementación de un Sistema de Gestión de Seguridad de la Información crezca a escala en concordancia con las necesidades de la organización según indica la NTPISO/IEC 27001:2014, (2014).

El Proyecto Especial Camélidos Sudamericanos – PECSA, es una Institución Descentralizada del Gobierno Regional Puno, que en el presente año viene ejecutando el Proyecto de Inversión Pública “Mejoramiento de la cadena de valor de la fibra de alpaca en la Región Puno”, cuyo objetivo, es establecer una red de entrada y salida de la información relacionada a la producción alpaquera, que permitirá como visión unir las 12 provincias dedicadas a esta actividad productiva importante y sobresaliente en la Región Puno.

La realidad, muestra que el manejo de la información actualizada fue deficitario y por lo tanto las decisiones técnicas y económicas no fueron las adecuadas. Por tanto, la propuesta de un Sistema de Gestión de Seguridad de la Información, responsable y actualizado, determinará el éxito del desarrollo de la actividad productiva debido a una apropiada toma de decisiones.

1.2. Formulación del Problema

1.2.1. Problema General.

¿Cómo establecer un Sistema de Gestión de Seguridad de la Información en el Proyecto Especial Camélidos Sudamericanos del Gobierno Regional Puno aplicando la Metodología MAGERIT, 2017?

1.2.2. Problemas Específicos.

a) ¿Cómo es la situación actual del Proyecto Especial Camélidos Sudamericanos del Gobierno Regional Puno en relación a la Seguridad de la Información, 2017?

b) ¿Cómo son los activos de la Seguridad de la Información en los principales procesos identificados en el Proyecto Especial

Camélidos Sudamericanos del Gobierno Regional Puno, aplicando la metodología Magerit, 2017?

c) ¿Cómo controla el Sistema de Gestión de la Seguridad de la Información en el Proyecto Especial Camélidos Sudamericanos del Gobierno Regional Puno, 2017?

d) ¿Cómo es la mejor propuesta de una política y controles de seguridad, en un Sistema de Gestión de Seguridad de la Información en el Proyecto Especial Camélidos Sudamericanos del Gobierno Regional Puno, basándonos con la metodología Magerit, 2017?

1.3. Justificación del estudio

1.3.1. Justificación y aportes del estudio.

Se entiende por información todo aquel conjunto de datos organizados en poder de una organización u institución pública que poseen un valor para la misma, independientemente de la forma en la que se guarde o retrasmita su origen o fecha de elaboración. La seguridad de la información, según la norma ISO 27001, consiste en la preservación de la confidencialidad, integridad y disponibilidad, además de los sistemas que se encuentran implicados en su tratamiento, dentro de la empresa.

1.3.2. Justificación Metodológica.

Por ello el presente estudio se respalda con los fundamentos teóricos de la Metodología MAGERIT Versión 3.0 este se basa en analizar el impacto que puede tener para la empresa en la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que

pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas como: Libro I: El método, Libro II: Catalogo de elementos y Libro II: Guía de Técnicas. Por lo tanto, esta metodología es muy útil para aquellas instituciones públicas o privadas que inicien con la gestión de la seguridad de la información, por lo tanto, permite enfocar los esfuerzos en los riesgos que puede resultar más críticos para una empresa, es decir aquellos relacionados con los sistemas de información. Así se estará alineando con los estándares en ISO ya que su implementación se convierte en el punto de partida para una certificación o para mejorar los Sistemas de Gestión.

1.3.3. Justificación Social

Se mejoraría de esta forma la comunicación y el clima tecnológico entre los trabajadores del Proyecto Especial Camélidos Sudamericanos (PECSA) para una adecuada toma de decisiones en la venta de fibra y reproductores de alpacas, haciendo participe a todos en el buen funcionamiento del Sistema de Gestión de la Seguridad de la información y además permitiendo que la información deje de ser una actividad poco organizada y con escaso apoyo por los trabajadores para ser un conjunto de actividades metódicas y controladas.

1.4. Objetivos de la Investigación

1.4.1. Objetivo General

Proponer un Sistema de Gestión de Seguridad de la Información, aplicando la metodología MAGERIT para el Gobierno Regional Puno, Caso: Proyecto Especial Camélidos Sudamericanos – PECSA, 2017.

1.4.2. Objetivos específicos

a) Conocer la situación actual del Proyecto Especial Camélidos Sudamericanos (PECSA) del Gobierno Regional Puno, respecto a la Seguridad de la Información, 2017.

b) Conocer los activos de la Seguridad de la Información, en el Proyecto Especial Camélidos Sudamericanos (PECSA) del Gobierno Regional Puno aplicando la metodología Magerit, 2017.

c) Conocer los controles del Sistema de Gestión de la Seguridad de la Información en el Proyecto Especial Camélidos Sudamericanos (PECSA) del Gobierno Regional Puno, 2017.

d) Conocer una Política y Manual del Sistema de Gestión de la Seguridad de la Información en el Proyecto Especial Camélidos Sudamericanos (PECSA) del Gobierno Regional Puno, basándonos con la metodología Magerit, 2017.

II. MARCO TEÓRICO

2.1. Antecedentes de la Investigación

En la búsqueda que se realizó con la finalidad de obtener más información acerca del tema, se han encontrado los siguientes trabajos de los cuales se asemejan a la presente investigación:

2.1.1. Antecedentes Nacionales

a) Se encontró el estudio realizado por **García Paredes, Adrian (2016).** En su tesis llamada: **"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, APLICADO A LOS RIESGOS ASOCIADOS A LOS ACTIVOS DE INFORMACIÓN EN LA EMPRESA NET – CONSULTORES S.A.C", UNIVERSIDAD NACIONAL DE SAN MARTIN – TARAPOTO.**

El investigador en su trabajo de investigación tuvo como objetivo fundamental, diseñar un SGSI para la empresa NET-Consultores bajo la Norma ISO/IEC 27001 con el fin de clasificar la información, identificar vulnerabilidades y amenazas en el área de informática; valorar los riesgos y con base en estos definir controles y políticas de seguridad que deben ser de conocimiento de la empresa, instrucciones de los procedimientos a realizarse y la documentación que se debe desarrollar en todo el proceso para la posterior implementación del SGSI, aplicando el modelo PDCA (Planificar, hacer, verificar y actuar).

La metodología utilizada es el desarrollo de la primera fase se aplica la metodología MAGERIT con la cual se realiza el análisis de riesgos que es uno de los procesos más

importantes que se debe realizar dentro de la empresa ya que permite identificar y analizar cada uno de los procesos y determinar los riesgos a los cuales esta expuestos cada uno de ellos. Además, permite identificar amenazas y vulnerabilidades.

Finalmente, a las conclusiones que llego el investigador es lograr diseñar el Sistema de Gestión de Seguridad de la Información para la empresa NET-Consultores S.A.C. utilizando la metodología MAGERIT; lo cual fue necesario para establecer Políticas de Seguridad de Información que contengan lineamientos para una correcta administración de la información con el fin de garantizar la seguridad de los activos esenciales e importantes para la empresa. Por lo tanto, se logró minimizar los riesgos asociados a los activos de información y finalmente se cumplido con el objetivo general donde se determinó que si influye significativamente la implementación de un Sistema de Gestión de Seguridad de la Información sobre el impacto de los riesgos asociados a los activos de información en la empresa NET–Consultores S.A.C.

b) Se encontró la tesis realizado por **Aguirre Mollehuanca y Daid Arturo (2014).** En su tesis llamada: **“DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA SERVICIOS POSTALES DEL PERÚ S.A.”, PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ – LIMA.**

El investigador en su trabajo de investigación tuvo como objetivo exigir la implementación de la norma técnica peruana NTP-ISO/IEC 27001:2008 en las entidades públicas nace de la necesidad de gestionar adecuadamente la seguridad de la información en cada una de estas empresas. Sin embargo, el

desconocimiento de estos temas por parte de la alta dirección, ha ocasionado que no se tomen las medidas necesarias para asegurar el éxito de este proyecto en el tiempo estimado por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), entidad responsable de apoyar a las entidades públicas durante el proceso de implementación de la norma.

La metodología empleada fue la tradicional SDLC que se refiere a las siguientes fases: Viabilidad, requerimientos, diseño, desarrollo e implementación.

Finalmente a las conclusiones a las que llego él investigador es que sin el apoyo de la alta gerencia para el Diseño de este Sistema de Gestión de Seguridad de la Información que fue imprescindible, ya que fue necesaria su intervención para ayudar a concientizar a los jefes de área y dueños de los procesos a participar de las entrevistas de levantamiento de información y ayudó a que entendieran que el SGSI no solo busca proteger la información digital, sino toda la información crítica del negocio independientemente del medio que la contenga. También es necesario difundir las normas de seguridad existentes y establecer charlas de capacitación y concientización en toda la empresa, esto debido a la poca cultura de seguridad que existe en la organización, desde las planas gerenciales hasta el personal operativo, incluyendo al personal de seguridad, debido a que se ha detectado que existen controles normados; sin embargo, estos no son conocidos por el personal y no existen métricas que permitan monitorear el cumplimiento de estas normas.

c) Se encontró la tesis realizado por **Villena Aguilar, Moises Antonio (2006).** En su tesis llamada: **“SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA UNA**

INSTITUCIÓN FINANCIERA" – PERÚ. PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ – LIMA.

El investigador en su trabajo de investigación tuvo como objetivo fundamental, establecer los principales lineamientos para poder implementar de manera exitosa, un adecuado modelo de sistema de gestión de seguridad de información (SGSI) en una institución financiera en el Perú, el cual apunte a asegurar que la tecnología de información usada esté alineada con la estrategia de negocio y que los activos de información tengan el nivel de protección acorde con el valor y riesgo que represente para la organización.

La metodología utilizada en este análisis, donde se procedió a realizar una revisión del estándar australiano AS/NZS 4360:2004 para aspectos de administración de riesgos, el cual forma parte primordial dentro de un Sistema de Gestión de Seguridad de la Información.

Finalmente, a las conclusiones a las que llegó el investigador es implantar una adecuada gestión de seguridad de información en una institución financiera, el primer paso que se tuvo es obtener el apoyo y soporte de la alta gerencia, haciéndolos participes activos de lo que significa mantener adecuada y protegida la información de la institución financiera. Al demostrarles lo importante que es la protección de la información para los procesos de negocio, se debe esperar de la alta gerencia su participación continua. Este apoyo luego se debe transmitir a los dueños de procesos de negocio más importantes de la institución financiera, que generalmente son jefes de áreas. Dándoles a conocer la importancia de la seguridad de información en los procesos que manejan, se espera el apoyo de todo el personal a su cargo. Es recién en este punto donde entran a tallar todos los

lineamientos del modelo de gestión expuesto, el cual se reflejará en las políticas, normas, estándares y procedimientos de seguridad, soportados por la tecnología de información de la institución. De nada sirve contar con los últimos adelantos tecnológicos, si no se da la importancia debida a la protección de la información, la cual se verá reflejada en el cumplimiento de todas las políticas de seguridad de información, siempre actualizadas de acuerdo a los cambios constantes en los negocios propios de una institución financiera.

2.1.2. Antecedentes Internacionales

a) Se encontró en el estudio realizado por **Tola Franco, Diana Elizabeth (2015)**. En su tesis llamada: **"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA DE CONSULTORÍA Y AUDITORÍA, APLICANDO LA NORMA ISO/IEC 27001", ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL – ECUADOR.**

El investigador en su trabajo de investigación tuvo como objetivo General: Lograr la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la norma ISO 27001:2005 para preservar la confidencialidad, integridad y disponibilidad de la información que maneja la empresa A y C Group S.A.

La metodología que utilizó es MAGERIT donde le permite enfocar los esfuerzos en los riesgos que pueden ser más críticos para la empresa, aquellos relacionados con los sistemas de información.

Finalmente, a las conclusiones que llego la

investigadora es establecer los objetivos y políticas del sistema de gestión de seguridad de la información, ya que estos van delineando el camino hacia donde la organización desea dirigirse para preservar la confidencialidad, integridad y disponibilidad de la información y por lo tanto es relevante la participación de la alta gerencia. Con la adopción de la metodología MAGERIT para el análisis de riesgos, le permitió identificar de manera oportuna la probabilidad y el impacto de que se materialicen los riesgos y de esta manera poder establecer controles que nos ayuden a prevenirlos. Una vez identificados los riesgos a los que están expuestos los activos de información, es necesario implementar controles o salvaguardas, con la finalidad de proteger estos activos y lograr minimizar la probabilidad de que se materialicen los riesgos o el impacto que pueden tener sobre la organización. Dentro del ciclo de un Sistema de Gestión de Seguridad de la Información, basado en ISO 27001, se encuentra la mejora continua, lo cual hace que sea muy importante que la organización se asegure de crear procedimientos para el monitoreo y revisión del sistema, los mismos que deben cubrir incidentes de seguridad, auditorías internas y revisiones gerenciales.

b) Se encontró en el estudio realizado por **Guamán Seis, Joseph Alexander (2015)**. En su tesis llamada: **"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES MILITARES", ESCUELA POLITÉCNICA NACIONAL – ECUADOR.**

El investigador en su trabajo de investigación tuvo como objetivo: Diseñar un Sistema de Gestión de Seguridad de la Información para Instituciones Militares, que incorpore estándares internacionales ajustados al campo militar y nuevas tecnologías de la información y comunicaciones con

el fin de contribuir a la modernización de las Instituciones Militares.

La metodología utilizada se sustentó en tres fases fundamentales, la primera el estudio del diagnóstico, la segunda la factibilidad; y la tercera el diseño de un Sistema de Gestión de Seguridad de la Información para Instituciones Militares, tomando como referencia la Norma ISO 27001:2005 y usando una combinación de metodologías para la evaluación de los riesgos que ayude a la toma de decisión sobre las opciones de tratamiento de riesgo adecuado.

Finalmente, a las conclusiones que llego el investigador fue que las Instituciones Militares, actualmente no disponen de un Sistema de Gestión de Seguridad de la Información para resguardar los activos de información que posee la institución, lo que dificulta mantener la información de acuerdo a las normas de la ISO 27001:2005. Para ello se realizó una encuesta para determinar cómo se encuentra la seguridad de la información en función a los objetivos definidos y aplicando un cuestionario estructurado con preguntas cerradas que cubren todos los aspectos de riesgos, incluso las amenazas a la confiabilidad, integridad y la disponibilidad de los datos que están basados en los objetivos de control de la ISO 27001:2005 para luego realizar el establecimiento del Diseño de un Sistema de Gestión de Seguridad de la Información para las Instituciones Militares; para así identificar el riesgo, amenazas y vulnerabilidades.

c) Se encontró en el estudio realizado por **Juan David Aguirre Cardona y Catalina Aristizabal Betancourt, (2013).** En su tesis llamada: **“DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL GRUPO EMPRESARIAL LA OFRENDA”, UNIVERSIDAD**

TECNOLÓGICA DE PEREIRA – COLOMBIA.

El investigador en su trabajo de investigación tuvo como objetivo principal: Diseñar un Sistema de Gestión de Seguridad de la Información para el Grupo Empresarial La Ofrenda.

La metodología aplicada se realizará con los siguientes paso que será tomados de la siguiente manera: Estudio de los diferentes riesgos y amenazas, con el propósito de documentar y argumentar la investigación, el desarrollo e implementación del sistema de seguridad de la información, Diseño de encuestas y entrevistas a personal con manejo de procesos y sub procesos importantes de la empresa, Validación de los riesgos encontrados, Diseño del sistema de gestión de la seguridad de la información y las Pruebas y validación del SGSI.

Finalmente, a las conclusiones que llego los investigadores es que actualmente se vive en una época en la que la información y los datos poseen una importancia decisiva en la gran mayoría de organizaciones, convirtiéndose así en su activo más importante. Es de opinar que una vez identificados los riesgos, se procede a desarrollar los controles para el SGSI. En el desarrollo del presente trabajo de grado, se utilizó tanto Cobit 4.1 como el estándar ISO/IEC 27001:2005 y el ISO/IEC 27002:2005 para armar nuestro marco de control y poder definir los controles a seguir para el aseguramiento de la información de la organización. Con un SGSI como el expuesto en este trabajo de grado se pueden solucionar problemas como: Brindar un nivel aceptable de seguridad con relación a la información que maneja la empresa, evitando incidentes que puedan afectar en la operativa diaria de la misma y como conclusión final, se debe

tener en cuenta que hay que recalcar que de nada sirve contar con un SGSI, que consideren todos los posibles riesgos y controles para mitigarlos o contar con toda la tecnología posible para asegurar la información de la compañía si no se da una debida importancia a la seguridad de la información por parte de la alta gerencia y no se cumplen las políticas y procedimientos establecidos por parte del personal de la empresa.

2.2. Bases Teóricas de las Variables

2.2.1. Sistema de Gestión de Seguridad de Información.

Según la **NTP-ISO/IEC 27001:2014, (2014)** En la actualidad, las empresas se enfrentan a muchos riesgos e inseguridades procedentes de focos diversos. Esto quiere decir que los activos de información de las empresas, uno de sus valores más importantes, se encuentran ligados o asociados a riesgos y amenazas que explotan una amplia tipología de vulnerabilidades.

La seguridad de estos activos de información está en función de la correcta gestión de una serie de factores como: la capacidad, la elaboración de un plan de contingencia frente a los incidentes, el análisis de riesgos, las competencias, el grado de involucración de la Dirección, las inversiones en seguridad y el grado de implementación de controles.

Según **Gómez Fernández and Fernández Rivero (2014)** definen a un Sistema de Gestión de Seguridad de la Información (SGSI) que es un conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la

seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización.

Su implantación supone el establecimiento de procesos formales y una clara definición de responsabilidades en base a una serie de políticas, planes y procedimientos que deberán constar como información documentada.
Fundamentalmente se distinguirán dos tipos de procesos:

1. Procesos de gestión. Controlan el funcionamiento del propio sistema de gestión y su mejora continua.

2. Procesos de seguridad. Se centran en los aspectos relativos a la propia seguridad de la información.

2.2.2. Organización de la seguridad de la información.

Según la **NTP-ISO/IEC 27001:2014, (2014)** Se debe establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización. Todas las responsabilidades de seguridad de la información deben ser definidas y asignadas.

Según **Gómez Fernández y Fernández Rivero, (2014)** define dos objetivos:

a. Organización interna, estableciendo el marco organizativo para la gestión de la seguridad de la información. Incluye los siguientes controles:

- ✓ Roles y responsabilidades en seguridad de la información. Es necesario definir y comunicar los roles y responsabilidades que se exigirán a cada persona implicada en la gestión de la seguridad de la

información, incluyendo empleados y terceras partes (usuarios externos, proveedores, etc.).

- ✓ Segregación de tareas. Puede ser necesario separar las diversas áreas de responsabilidad para evitar usos o accesos indebidos a la información y los activos que la gestionan. Esta segregación puede resultar difícil de aplicar en organizaciones pequeñas, pero el principio debería aplicarse en la medida en que sea posible y práctico.

- ✓ Contacto con las autoridades. Pueden darse casos en los que sea necesario disponer de contacto con las autoridades u otros organismos de control. Por ejemplo, para notificar problemas de seguridad, o con las fuerzas y cuerpos de seguridad en caso de incidentes graves.

- ✓ Contacto con grupos de interés especial. Conviene mantener contactos con grupos y foros especializados en seguridad de la información, de manera que se reciban noticias y recomendaciones que permitan mejorar la seguridad de la información y permanecer alerta ante nuevas amenazas.

- ✓ Seguridad de la información en la gestión de proyectos. La seguridad de la información debe considerarse como un aspecto más dentro de la gestión de un proyecto de la organización, independientemente del tipo que sea (proyecto de negocio, proyectos internos, proyectos de IT, etc.). Así, en el ciclo de vida de un proyecto deberán incluirse los objetivos de seguridad, la evaluación de riesgos y la aplicación de controles necesarios.

b. Los dispositivos móviles y el teletrabajo, que tiene como objetivo proteger la información almacenada en los dispositivos móviles y en las condiciones empleadas en el teletrabajo. Se incluyen dos controles:

- ✓ Política de dispositivos móviles. Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.

- ✓ Teletrabajo. Cuando se permita el teletrabajo, deben aplicarse los mismos niveles de seguridad que en el trabajo local. Para ello, además de las medidas de seguridad que se tengan a nivel local, se deben considerar las medidas de seguridad propias de los canales de comunicaciones empleados y las de seguridad física de las ubicaciones remotas.

2.2.3. Seguridad de los recursos humanos.

Según la **NTP-ISO/IEC 27001:2014, (2014)** es asegurar que los empleados y contratistas entienden sus responsabilidades y son convenientes para los roles para los que se les considera. Las verificaciones de los antecedentes de todos los candidatos a ser empleados deben ser llevadas a cabo en concordancia con las leyes, regulaciones y ética relevantes, y debe ser proporcional a los requisitos del negocio, la clasificación de la información a la que se tendrá acceso y los riesgos percibidos. Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.

Según **Gómez Fernández y Fernández Rivero, (2014)** dice que la gran parte de los incidentes de seguridad provienen

de errores humanos, por lo tanto se debe de concienciar y capacitar al personal en el desarrollo de sus actividades y, especialmente, en lo relacionado con la seguridad de la información, considerando tres etapas distintas: Antes del empleo, durante el empleo y una vez finalizada la relación laboral:

- ✓ **Antes del empleo**, para asegurar que los empleados y contratistas conocen y entienden sus responsabilidades. Los controles son dos:

  - Investigación de antecedentes. Es interesante verificar la formación y experiencia previa del candidato al puesto de trabajo, por ejemplo, verificando la exactitud de lo detallado en el currículum respecto de los títulos o solicitando referencias de anteriores puestos de trabajo.

  - Términos y condiciones del empleo. Los contratos deberán incluir, además de los términos del acuerdo laboral, las obligaciones y responsabilidades de las dos partes en lo relativo a seguridad de la información.

- ✓ **Durante el empleo**, para asegurar que los empleados y contratistas son conscientes de las políticas de seguridad establecidas en la organización y las cumplen. Este objetivo incluye tres controles:

  - Responsabilidades de gestión. Es la dirección la que debe exigir la aplicación de seguridad de la información de acuerdo con las políticas establecidas en la organización.

  - Concienciación, educación y capacitación en seguridad de la información. El personal afectado debe ser consciente del papel que juega en la gestión de la seguridad de la

información y su importancia, así como debe estar capacitado para llevar a cabo las tareas relacionadas. Para ello es recomendable establecer planes de concienciación y formación que se renueven periódicamente.

- Proceso disciplinario. Deben existir y comunicarse aquellas medidas disciplinarias que la organización podría llevar a cabo ante el incumplimiento de las políticas definidas.

✓ **Finalización del empleo** o cambio en el puesto de trabajo, para proteger los intereses de la organización ante el cese de una relación laboral o un cambio en la misma. Se incluye un único control:

- Responsabilidades ante la finalización o cambio. Las responsabilidades deben estar establecidas y ser conocidas en caso de cese o cambio de puesto de algún empleado, incluyendo aquellas que se extiendan más allá de la relación laboral, como puede ser el deber de confidencialidad.

2.2.4. Gestión de activos.

Según la **NTP-ISO/IEC 27001:2014, (2014)** nos indica que se tiene que identificar los activos de la organización y definir responsabilidades de protección apropiada. Información, otros activos asociados con información e instalaciones de procesamiento de información deben ser identificados y un inventario de estos activos debe ser elaborado y mantenido.

Según: **Gómez Fernández y Fernández Rivero, (2014)** define que las responsabilidad sobre los activos. Para una adecuada protección de los activos, el primer paso será proceder a su identificación y a la asignación de responsabilidades sobre los mismos. Se incluyen cuatro controles:

- ✓ **Inventario de activos.** Es necesario proceder a la identificación de los activos que dan soporte a los procesos de negocio y a la información de la organización, elaborando para ello un inventario que permanezca actualizado.

- ✓ **Propiedad de los activos.** Se debe establecer, para cada uno de los activos identificados, un propietario, entendiendo como tal el responsable de su seguridad.

- ✓ **Uso aceptable de los activos.** La organización debe establecer y comunicar las normas para la utilización aceptable de la información y de los activos que la soportan, de manera que sean conocidas y aplicadas por todas las partes afectadas, tanto internas como externas, cuando sea necesario.

- ✓ **Devolución de activos.** Se deberá establecer un control para que todos los empleados y terceras partes devuelvan los activos cedidos por la entidad una vez finalizada la relación laboral.

2.2.5. Control de acceso.

Según la **NTP-ISO/IEC 27001:2014, (2014)** define que se tiene que limitar el acceso a la información y a las instalaciones de procesamiento de la información. Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información. La asignación y uso de derechos de acceso privilegiado debe ser restringida y controlada.

Según **Gómez Fernández y Fernández Rivero, (2014)** indica que el control de acceso contiene todas las medidas encaminadas a gestionar y monitorizar los accesos a los recursos de información, en base a las políticas que la

organización determine, que deberán estar alineadas con los requisitos de negocio y de seguridad, y considerando tanto riesgos internos como externos.

- ✓ Requisitos de negocio para el control de acceso, para limitar el acceso a la información únicamente a quienes estén autorizados para ello. Incluye dos controles:

  – Política de control de acceso. Se deben establecer los objetivos de la organización y sus necesidades aplicando el principio del mínimo privilegio, es decir, que los usuarios tengan acceso únicamente a la información y medios de tratamiento que requieran para el desarrollo de su actividad profesional.

  – Acceso a las redes y a los servicios de red. Hay que establecer cómo se van a utilizar la red y sus servicios, y definir cómo se van a asignar los accesos, teniendo en cuenta lo definido en la política de controles de acceso.

- ✓ Gestión de acceso de usuario, de manera que únicamente los usuarios autorizados tengan acceso a la información, a los sistemas y a los servicios. Se incluyen los siguientes controles:

  – Registro y baja de usuario. Debe establecerse un proceso formal para el registro de usuarios, que puede contemplar la verificación de la identidad del usuario, la asignación de identificadores únicos de usuario, etc.

  – Provisión de acceso de usuario. Es necesario un proceso formal para asignar o revocar los accesos a sistemas y servicios, que permita evitar fallos y mantener información sobre los accesos concedidos en cada momento.

– Gestión de privilegios de acceso. Se debe tener especial cuidado con las cuentas con permisos de administración, ya que son un factor importante en los incidentes de seguridad. Para ello se debe controlar su uso y asignación, mediante autorizaciones, registros, requisitos y condiciones de uso. Por ejemplo, no deberían utilizarse este tipo de cuentas para tareas rutinarias que no requieran ese nivel de acceso.

– Gestión de la información secreta de autenticación de los usuarios. La información secreta de autenticación (por ejemplo, contraseñas) debe custodiarse rigurosamente. Para ello los usuarios deben estar concienciados, firmar compromisos de mantener secreto sobre los mismos y, cuando sea necesario almacenarlos, deberá considerarse la necesidad del uso de mecanismos de cifrado. También se debe tener en cuenta la importancia de modificar la información secreta de autenticación que pudieran incorporar por defecto los nuevos sistemas.

– Revisión de los derechos de acceso de usuario. La necesidad de acceder a una determinada información o recurso puede variar a lo largo del tiempo. Por eso, es conveniente que los responsables realicen revisiones periódicas de los derechos de acceso asignados a los usuarios.

– Retirada o reasignación de los derechos de acceso. Los permisos de acceso deben suprimirse cuando finalice la relación laboral o contrato y modificarse cuando se produzcan cambios en los mismos. Es importante que cada usuario acceda, en todo momento, únicamente a la información que requiere para desarrollar su trabajo.

- ✓ Responsabilidades del usuario. Los usuarios deben ser conscientes y asumir la responsabilidad sobre el uso de los medios de autenticación que la entidad les facilita.

  - Uso de la información secreta de autenticación. Se deben establecer unas normas para la creación, uso correcto y custodia de la información secreta de autenticación.

- ✓ Control de acceso a sistemas y aplicaciones. El objetivo en este caso es prevenir el acceso no autorizado a los sistemas y aplicaciones. Para ello se incluyen cinco controles:

  - Restricción del acceso a la información. El hecho de que un usuario disponga de acceso a un sistema de información no implica que tenga acceso a toda la información y funciones del mismo. Para ello, los sistemas deberán disponer de perfiles que permitan limitar el acceso de los usuarios a las partes necesarias para desarrollar sus funciones.

  - Procedimientos seguros de inicio de sesión. El proceso de inicio de sesión debe llevarse a cabo de manera segura. Para ello se debe considerar la información que se ofrecerá en la pantalla de login, el contenido de los mensajes de error, la limitación de intentos de acceso fallidos, etc.

  - Sistema de gestión de contraseñas. Cuando se utilicen contraseñas, estas deben cumplir unos mínimos requisitos de complejidad y ser modificadas periódicamente, buscando un equilibrio entre estos requisitos y la capacitación del personal que tendrá que usarlos. En ocasiones, puede no ser buena idea pasar

rápidamente de un sistema de gestión de contraseñas con unas reglas sencillas a otro mucho más complejo, sino que este proceso deberá llevarse a cabo de manera progresiva.

– Uso de utilidades con privilegios del sistema. Los sistemas disponen de funciones y aplicaciones que permiten deshabilitar o reducir la capacidad de las medidas de seguridad implantadas. Por ello, es recomendable que los permisos de administración de los equipos recaigan únicamente sobre el personal capacitado para su gestión.

– Control de acceso al código fuente de los programas. Cuando se desarrolla software, el código fuente del mismo pasará a ser un activo a proteger, debiendo limitarse el acceso al mismo y estableciendo medidas para controlar los cambios.

2.2.6. Seguridad física y ambiental

Según la **NTP-ISO/IEC 27001:2014, (2014)** dice impedir el acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la organización. Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado. Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.

Según **Gómez Fernández y Fernández Rivero, (2014)** dice que la seguridad de la información y los activos no solo depende de un conjunto de medidas de seguridad tecnológicas sino de una adecuada protección física que permita prevenir

incidentes que provoquen accesos o daños físicos, así como interferencias. Así, será necesario determinar un perímetro de seguridad física, para lo que la norma desarrolla dos objetivos.

- ✓ **Áreas seguras**. Será necesario definir medidas de seguridad para prevenir los accesos físicos no autorizados, los daños e interferencias en las instalaciones y en la información de la organización. Se incluyen los siguientes controles:

  – Perímetro de seguridad física. Se debe delimitar el perímetro de seguridad física aplicando medidas proporcionadas a la criticidad de los medios que contienen. Deberán instalarse barreras físicas, puestos de control de acceso, puertas, etc., donde sea conveniente. También es importante tener en cuenta la importancia de no facilitar información al público sobre las instalaciones y su contenido.

  – Controles físicos de entrada. Se debe restringir el acceso a las distintas zonas identificadas únicamente a personal autorizado. Se debe valorar la posibilidad de aplicar sistemas de registro de entrada y salida, por ejemplo, en los CPD, o una recepción para el caso de oficinas. En el caso de proveedores o personal externo, será conveniente que permanezcan adecuadamente identificados.

  – Seguridad de oficinas, despachos y recursos. Se deben identificar y aplicar medidas apropiadas para la seguridad de las oficinas y lugares de trabajo habitual. Por ejemplo, debe velarse porque las pantallas e impresoras se sitúen en zonas no visibles o accesibles por parte de personal no autorizado.

– Protección contra las amenazas externas y ambientales. Considerando el daño que podrían provocar este tipo de amenazas, conviene disponer de planes de acción para responder a las mismas. Por otra parte, la legislación obliga a disponer de planes de autoprotección o de emergencias que incluirán este tipo de actuaciones.

– El trabajo en áreas seguras. Además de establecer medidas de protección física, se definirán e implantarán procedimientos para el trabajo a desarrollar en las áreas seguras, por ejemplo, el acompañamiento y supervisión de visitantes, revisión de las zonas, prohibición de tomar imágenes, etc.

– Áreas de carga y descarga. Al tratarse de puntos a través de los cuales podría vulnerarse la seguridad física, deberán controlarse las zonas de carga y descarga y se debe valorar la necesidad de inventariar y revisar los materiales entregados.

✓ **Seguridad de los equipos**, para que la actividad de la organización no se vea interrumpida por daños en los equipos, robo de activos o pérdidas de los mismos. Los controles incluidos son:

– Emplazamiento y protección de equipos. La ubicación de los equipos debe ser tal que se eviten daños por amenazas ambientales y el acceso no autorizado a los mismos.

– Instalaciones de suministro. Al menos para los equipos más sensibles se debe valorar la posibilidad de disponer de equipos que prevengan daños por alteraciones en el suministro eléctrico, por ejemplo, picos de tensión o fallos del suministro.

– Seguridad del cableado. Se debe proteger el cableado, tanto de suministro eléctrico como de transporte de datos, para evitar daños, accidentales o intencionados, o la interceptación de comunicaciones.

– Mantenimiento de los equipos. Es aconsejable desarrollar tareas periódicas de mantenimiento preventivo de los equipos de manera que no decaiga su rendimiento y se eviten incidentes de seguridad. Es aconsejable, cuando existan, seguir las recomendaciones de los fabricantes.

– Retirada de materiales propiedad de la empresa. Se debe evitar la salida de activos (información, equipos, aplicaciones, etc.) y cuando sea absolutamente necesario se deberá disponer de la debida autorización y control.

– Seguridad de los equipos fuera de las instalaciones. Cuando un equipo abandona el perímetro de seguridad física establecido en las instalaciones bajo el control de la organización, pueden surgir nuevos riesgos. Por ello, será necesario identificar e implantar las medidas que los mitiguen.

– Reutilización o eliminación segura de equipos. Los equipos almacenan información que debe ser eliminada de forma segura cuando son retirados o se van a reutilizar. Para ello deberán aplicarse mecanismos de borrado y/o destrucción seguros.

– Equipo de usuario desatendido. Cuando un usuario abandona su puesto de trabajo se corre el riesgo de sufrir una suplantación del mismo. Para evitarlo, deben aplicarse

medidas de bloqueo del puesto de trabajo y cierre de sesiones de trabajo abiertas.

– Política de puesto de trabajo despejado y pantalla limpia. Lo puestos de trabajo deberían permanecer despejados de todo material de trabajo que no esté siendo utilizado. Para ello deberían habilitarse armarios o cajoneras con dispositivo de cierre.

2.2.7. Seguridad de las operaciones.

Según la **NTP-ISO/IEC 27001:2014, (2014)** indica que se tiene que asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras. Realizando copias de respaldo de información, del software y de las imágenes del sistema; así como también reglas que gobierne la instalación de software por parte de los usuarios que deben ser establecidas e implementadas.

Según **Gómez Fernández y Fernández Rivero, (2014)** dice que debe contener una serie de controles con un fuerte componente técnico. Siendo importante seleccionar, para cada control, aquellos aspectos que puedan aportar un mayor beneficio a la organización. Define siete objetivos:

1. Procedimientos y responsabilidades operacionales. La organización determinará aquellas actividades para las que es necesario que se desarrollen procedimientos, en los que se determine quién debe realizar cada tarea. Los controles son:

   - Documentación de procedimientos de la operación. Es importante que en la organización quede claro que se deben llevar a cabo determinadas tareas y quién es el

responsable de ejecutarlas. Esta información quedará reflejada en procedimientos, que deberán permanecer actualizados en todo momento.

- Gestión de cambios. Las organizaciones están sujetas a constantes cambios, tanto internos como en el entorno. Estos cambios pueden afectar a la gestión de la seguridad de la información, por lo que es importante disponer de un proceso que permita evaluar el impacto de estos cambios y definir las medidas oportunas en cada caso.

- Gestión de capacidades. Se monitorizará el uso de recursos y se realizarán previsiones futuras, planificando la dotación de recursos cuando sea necesario, evitando pérdidas de disponibilidad o rendimiento de los sistemas por falta de capacidad.

- Separación de los recursos de desarrollo, prueba y operación. Cuando se desarrollan sistemas, es importante que se separen los entornos de desarrollo e integración de los de producción, para evitar cambios indeseados o problemas de disponibilidad. Asimismo, el código fuente o las herramientas de desarrollo no deben estar disponibles en el entorno de producción, ya que se verían sujetos a graves riesgos de seguridad.

2. Protección contra software malicioso (malware). Cada día son más numerosas las vías por las que pueden transmitirse los códigos maliciosos. Por eso, además de proteger el perímetro lógico, se deben proteger los equipos.

   - Controles contra el código malicioso. Debe disponerse de sistemas de detección de código malicioso en

servidores y puestos de trabajo, siendo necesario que permanezcan debidamente actualizados frente a las amenazas que surgen día a día. Además, los usuarios deben estar preparados para saber responder ante posibles incidencias detectadas por estos sistemas.

3. Copias de seguridad. Implantar y mantener una política de copias de seguridad permite asegurar la disponibilidad e integridad de la información ante incidentes. Este objetivo incluye un único control:

   - Copias de seguridad de la información. La implantación de un sistema de copias de seguridad debería comenzar por identificar las necesidades de recuperación para los distintos conjuntos de información, estableciéndose así los requisitos de periodicidad. Por otra parte, tanto las políticas como los mecanismos implantados para la realización de copias deben revisarse y probarse periódicamente para comprobar su validez. Otra cuestión a tener en cuenta es la necesidad de mantener copias de seguridad en una ubicación alternativa a la principal que permita recuperar la información en caso de desastre. No solo deben de mantenerse las propias copias, sino también los medios que permitan su restauración en un momento dado.

4. Registros y supervisión. Para cada sistema de información, deberían analizarse y definirse las necesidades de trazabilidad, aplicando posteriormente los sistemas de registro que permitan determinar la autoría de determinadas acciones. Los controles que se incluyen aquí son:

   - Registro de eventos. En cada sistema pueden contemplarse distintos eventos que puede ser necesario

registrar; intentos de acceso exitosos y fallidos, desconexiones del sistema, acciones ejecutadas, alertas por fallos en el sistema, etc. Asimismo, se debe determinar el tiempo de retención para estos registros, atendiendo a requisitos legales y de negocio. Por último, es importante revisar los registros, de manera que puedan detectarse potenciales problemas antes de que estos ocurran.

- Protección de la información de los registros. Se debería velar por la integridad y disponibilidad de los registros, por ejemplo, aplicando segregación de tareas, para que los usuarios del sistema no puedan manipular los registros, y mediante la realización de copias de seguridad.

- Registros de administración y operación. No solo debe registrarse la actividad de los usuarios estándar de los sistemas, sino también aquellas actividades llevadas a cabo por los que disponen de privilegios de administración. Deberá prestarse especial atención a la protección de los mismos, ya que en estos casos el riesgo de manipulación o borrado serán mayores.

- Sincronización del reloj. Realizar un análisis de un determinado evento suele conllevar el análisis de registros en diversos sistemas. Si estos sistemas no tienen la hora sincronizada, será muy complicado, o imposible, establecer la sucesión de eventos.

5. Control del software en explotación. Una falta de control sobre el software utilizado puede provocar problemas de compatibilidad, de licencia, así como de rendimiento de los equipos. Por ello se establece un control con este sentido.

- Instalación del software en explotación. Los cambios y nuevas instalaciones de software deberían probarse antes en entornos aislados, de manera que se asegure la compatibilidad con la actual infraestructura de la organización. Asimismo, se debe estar al día de las actualizaciones propuestas por los fabricantes, valorando en cada caso la necesidad de su instalación.

6. Gestión de la vulnerabilidad técnica. Periódicamente se descubren fallos de seguridad en el software, que son subsanados por los fabricantes mediante actualizaciones de seguridad.

   - Gestión de las vulnerabilidades técnicas. Existen varios métodos para la identificación de vulnerabilidades técnicas: la consulta de foros especializados, la información facilitada por los fabricantes y proveedores y la realización de procesos de hacking ético o pruebas de penetración. En cada caso se deberán valorar uno o varios métodos que permitan identificar vulnerabilidades en los sistemas y aplicar las medidas correctoras oportunas.

   - Restricción en la instalación de software. La instalación de software solo debería ser llevada a cabo por personal autorizado con la debida capacitación, limitándose la posibilidad de que los usuarios finales instalen o manipulen los paquetes de software instalados y proporcionándoles únicamente la funcionalidad que requieran para el desarrollo de sus funciones.

7. Consideraciones sobre la auditoría de los sistemas de información. Cuando se realicen auditorías que impliquen la

interacción con los sistemas, deben planificarse de manera que, consiguiendo los objetivos perseguidos, se interfiera lo mínimo posible en la actividad de la entidad.

- Controles de auditoría de sistemas de información. Aquellas auditorías ejecutadas para comprobar la validez de las medidas implantadas generalmente implican el uso de herramientas que pueden consumir una gran cantidad de recursos. Por ello, es conveniente realizarlas de manera controlada y en horarios o periodos de tiempo que no impacten en la operativa diaria.

2.2.8. Seguridad de las comunicaciones

Según la **NTP-ISO/IEC 27001:2014, (2014)** indica que se debe asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo. Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones como: Mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en acuerdos de servicios de red, ya sea que estos servicios se provean internamente o sean tercerizados.

Según **Gómez Fernández y Fernández Rivero, (2014)** dice que la gran mayoría de los intercambios de información se realizan a través de redes de comunicaciones. Por ello es importante proteger adecuadamente los medios de transporte de la información, considerando medidas de seguridad tanto para la red interna como para las comunicaciones con el exterior.

- ✓ Gestión de la seguridad de redes. Todas las organizaciones cuentan, al menos, con una red por la que se intercambia información, tanto a nivel interno como externo. En estas

comunicaciones intervienen distintos elementos que conviene proteger.

- Controles de red. La protección de las redes debe contemplar tanto la seguridad de los elementos físicos que le dan soporte (routers, switch, etc.) como la seguridad en el envío de datos. Además, se debe valorar la posibilidad de limitar los sistemas que podrán conectarse a la red y de registrar la actividad en la misma.

- Seguridad de los servicios de red. Se deben especificar los requisitos de la red en relación a la calidad del servicio y a las medidas de seguridad que debe implementar. Cuando los servicios de red se subcontraten, deberá exigirse a los proveedores la aplicación y cumplimiento de esas condiciones.

- Segregación en redes. Una posibilidad de limitar el impacto de los incidentes, los accesos no autorizados o la fuga de información, es la de separar las redes física o lógicamente. Para ello es conveniente, cuando se aplique, definir una estrategia de segregación de redes, por ejemplo, por servicios, por departamentos, o por una combinación de varios factores.

✓ Intercambio de información. Se debe proteger la información cuando se transfiere dentro de la propia organización, así como cuando se envía a otras entidades. Para ello se incluyen los siguientes controles:

- Políticas y procedimientos de intercambio de información. Se deberían establecer políticas y procedimientos para proteger la información que será

objeto de intercambio, considerando todos los medios por los que puede ser transportada: redes, soportes informáticos, documentos, etc. Las medidas de seguridad deberán definirse en función de la naturaleza del soporte.

- Acuerdos de intercambio de información. El intercambio de información con otras entidades debe llevarse a cabo bajo un acuerdo documentado en el que se establezcan las responsabilidades sobre el uso de la información, así como sobre las protecciones que se aplicarán.
- Mensajería electrónica. Deben establecerse normas para el uso seguro de los sistemas de mensajería, incluyendo correo electrónico, redes sociales, o sistemas de chat cuando el acceso a los mismos esté permitido.

- Acuerdos de confidencialidad o no revelación. Antes de comenzar el intercambio de información con terceras partes, deben obtenerse por escrito acuerdos de confidencialidad y de deber de secreto, en los que además se especifique el uso que se dará a esa información. El deber de secreto debe mantenerse incluso más allá de la relación profesional entre las dos entidades.

2.2.9. Cumplimiento.

Según la **NTP-ISO/IEC 27001:2014, (2014)** indica evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad. Como los registros deben ser protegidos de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada

de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio. Los gerentes deben revisar regularmente el cumplimiento del procesamiento de la información y de los procedimientos dentro de su área de responsabilidad con las políticas, normas y otros requisitos de seguridad apropiadas.

2.2.10. Sistema de Gestión

Fernández García (2006) Se entiende por Sistema de Gestión la estructura organizada, la planificación de las actividades, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos para desarrollar, implantar, llevar a cabo revisar y mantener al día la política de la empresa. En otras palabras, es un método sistemático de control de las actividades, procesos y asuntos relevantes para una organización, que posibilite alcanzar los objetivos previstos y obtener el resultado deseado, a través de la participación e implicación de todos los miembros de la organización y garantizando la satisfacción del cliente, de la sociedad en general y de cualquier parte interesada.

2.2.11. Seguridad de la Información

Según **Areitio Bertolín (2008)** La seguridad de la información es un proceso en el que se da cabida a un crecimiento número de elementos: aspectos tecnológicos, de gestión organizacionales, de recursos humanos, de índole económica, de negocios, de tipo legal, de cumplimiento, etc.; abarcando no sólo aspectos informáticos y de telecomunicaciones sino también aspectos físicos medioambientales, humanos, etc.

Según la Norma **ISO/IEC 27001:2013** Consiste en la preservación de su confidencialidad, integridad y

disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- ✓ **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- ✓ **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- ✓ **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

  Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

2.2.12. Gestión de la seguridad de la información

Según **Gómez Fernández y Fernández Rivero, (2014)** un Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización.

2.2.13. Metodología Magerit

Dirección General de Modernización Administrativa (2012) siguiendo la terminología de la normativa ISO 31000:2009, MAGERIT responde a lo que se denomina “Proceso de Gestión de los Riesgos”. En otras palabras, Magerit Implementa el Proceso de Gestión de riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

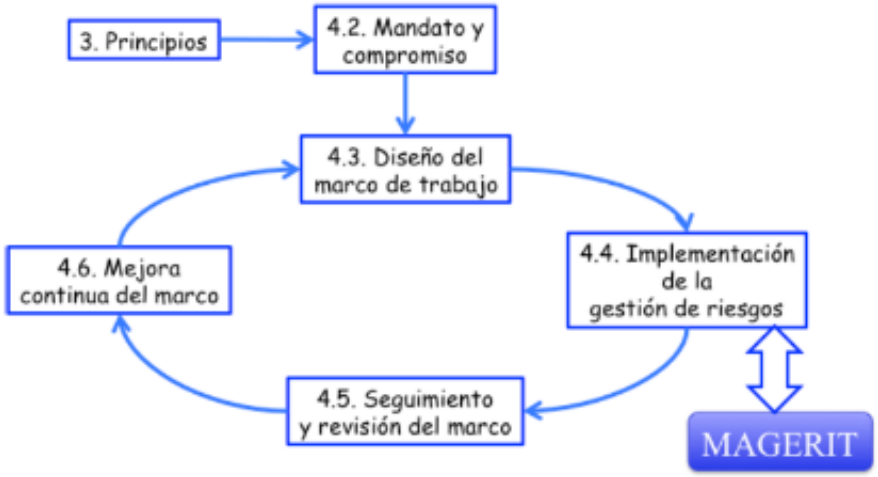


Figura 1: Marco de trabajo para la gestión de riesgos
Fuente: Libro I – Método (2012)

Según **Camila Bolaños and Rocha Galvis (2014)** La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de Administraciones públicas, MAGERIT, es un método formal para investigar los riesgos que soportan los sistemas de información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

MAGERIT, ha sido elaborada por un equipo interdisciplinar del Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos personales, SSITAD, del Consejo Superior de Informática.

Objetivos de MAGERIT

- ✓ Estudiar los riesgos que soportan un sistema de información y el entorno asociado a él.

- ✓ Propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización.

- ✓ Señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenas, obteniendo unos resultados.

- ✓ Permite recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o posibles perjuicios.

Con la aplicación de MAGERIT se permite:

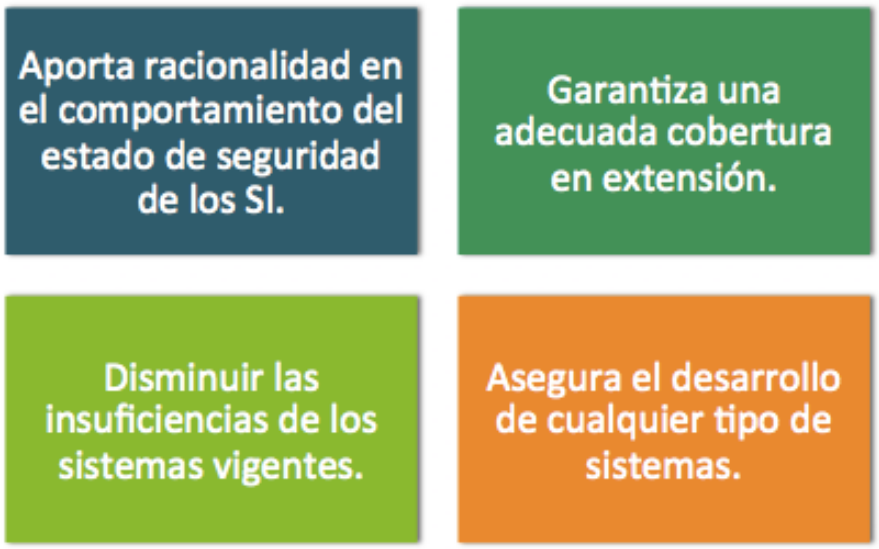


Figura 2: Aplicación de Magerit
Fuente: Auditoria de SI, María Camila Bolaños (2014)

Análisis de Riegos para identificar las amenazas que acechan a los distintos componentes pertenecientes o relacionados al Sistema de Información (activos); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener en la organización, obteniendo cierto conocimiento del riesgo que se corre.

Gestión de Riesgos basada en los resultados obtenidos en el análisis anterior, que permite seleccionar e implantar las medidas o "salvaguardas" de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

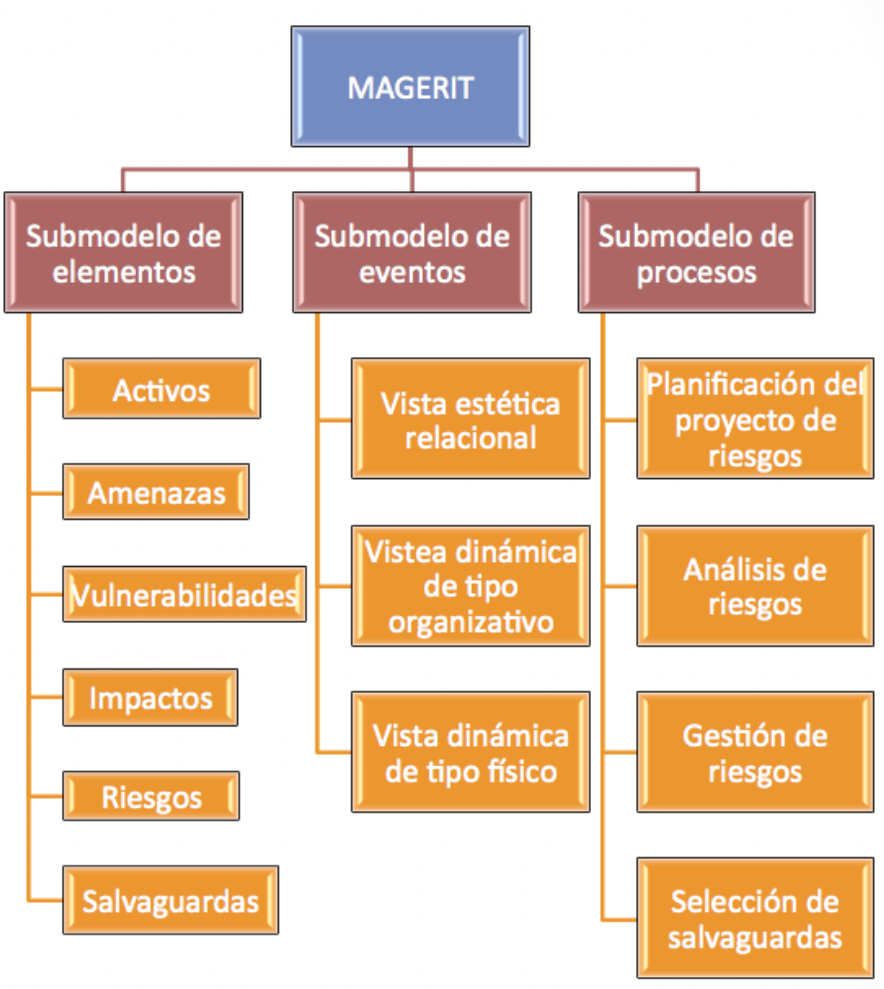


Figura 3: Estructura de Magerit
Fuente: Estructura del MAGERIT, María Camila y Mónica Rocha (2014)

Tipo de Técnicas

- ✓ Guía de aproximación
- ✓ Guía de procedimientos
- ✓ Guía de técnicas
- ✓ Guía para responsables del dominio
- ✓ Guía para desarrolladores de aplicaciones
- ✓ Arquitectura de información y especificaciones de interfaz para el intercambio de datos
- ✓ Referencia normativa

2.3. Definición de Términos Básicos

a) Activo: Un activo se define como aquel recurso del sistema (informático o no) necesario para que la organización alcance los objetivos propuestos; es decir, todo aquello que tenga valor y que deba ser protegido frente a un eventual percance, ya sea intencionado o no. Según esta definición, consideraremos como activos: los trabajadores, el software, los datos, los archivos, el hardware, las comunicaciones, etc. (Escrivá, 2013, p.9)

b) Amenaza: En Sistema de Información se entiende por amenaza la presencia de uno o más factores de diversa índole (personas, máquinas o sucesos) que de tener la oportunidad atacarían al sistema produciéndole daños provechándose de su nivel de vulnerabilidad. Hay diferentes tipos de amenazas de las que hay que proteger al sistema, desde la física como cortes eléctricos, fallos del hardware o riesgos ambientales hasta los errores intencionados o no de los usuarios, la entrada de software malicioso (virus, troyanos, gusanos) o el robo, destrucción o modificación de la información (Aguilera, 2010, p.13)

c) **Ataques:** Un ataque es una acción que trata de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre él e incluso tomar el control del mismo. Se trata de acciones tanto intencionadas como fortuitas que pueden llegar a poner en riesgo un sistema. De hecho, en alguna metodología como MAGERIT se distingue entre ataques (acciones intencionadas) y errores (acciones fortuitas) (Escrivá, 2013, p10).

d) **Calidad:** Los datos de carácter personal solo se pueden recoger para su tratamiento cuando estos sean adecuados, pertinentes y no excesivos para cumplir las finalidades del fichero. Estos datos no podrán tener un uso distinto al definido en su recogida. La única excepción para conservar o tratar datos con un uso distinto a la inicial es utilizarlos en momentos posteriores para fines históricos, estadísticos o científicos (Chicano, 2014, p.31).

e) **Ciclo de Denning:** Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información se utiliza el ciclo PDCA (conocido también como ciclo Deming), tradicional en los Sistemas de Gestión de la Calidad. El ciclo PDCA (Plan, Do, Check y Act.) es un concepto ideado originalmente por Shewhart, pero adaptado a lo largo del tiempo por algunos de los más sobresalientes personajes del mundo de la calidad. Esta metodología ha demostrado su aplicabilidad y ha permitido establecer la mejora continua en organizaciones de todas clases (Gómez y Álvarez, 2012, p.14).

f) **Confidencialidad:** La OCDE (Organización para la Cooperación y el Desarrollo Económico), en sus Directrices para la Seguridad de los Sistemas de Información define la confidencialidad como “el hecho de que los datos o informaciones estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada”. Para prevenir errores de confidencialidad debe diseñarse un control de accesos al sistema: quién puede acceder, a

qué parte del sistema, en que momento y para realizar qué tipo de operaciones (Aguilera, 2010, p10).

g) **Control:** medios para manejar el riesgo, incluyendo políticas, procedimientos, prácticas o estructuras organizacionales, que pueden ser administrativas, técnicas, de gestión o de naturaleza legal (Chicano, 2014, p.13).

h) **Datos:** Flujos de hechos en crudo que representan los eventos que ocurran en organizaciones o el entorno físico antes de organizarlos y ordenarlos en un formato que las personas puedan entender y usar (Laudon, 2012, p.G4).

i) **Diagnosticar:** El diagnóstico implica en sí mismos una comparación entre una situación presente, conocida mediante la investigación y otra situación ya definida o conocida previamente que sirve de referencia (Arteaga y Montaño, 2001, p.83).

j) **Disponibilidad:** La información ha de estar disponible para los usuarios autorizados cuando la necesiten.

Según **MAGERIT Libro II - Catálogo de Elementos (2012)** define la disponibilidad como “grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Situación que se produce cuando se puede acceder a un sistema de información en un periodo de tiempo considerado aceptable. La disponibilidad está asociada a la fiabilidad técnica de los componentes del sistema de información”.

Se deben aplicar medidas que protejan la información, así como crear copias de seguridad y mecanismos para restaurar los datos que accidental o intencionadamente se hubiesen dañado o destruido (Aguilera, 2010, p.11).

k) **Gestión:** Para gestionar de forma adecuada la Seguridad de la Información se han desarrollado un conjunto de estándares que se han convertido en el marco para establecer, implantar, gestionar y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI). Son las normas ISO/IEC 27000, desarrolladas por ISO (International Organization for Standarization) e IEC (International Electrotechnical Commission) (Escrivá, 2013, p.7).

l) **Hardware:** Es un término de origen anglosajón que hace referencia a cualquier componente físico tangible que trabaja o interactúa de algún modo en los equipos de cómputo; incluye tanto los elementos internos como el disco duro, la unidad CD-ROM y las unidades USB; asimismo, hace referencia al cableado, los circuitos, el gabinete, etcétera. Incluso se relaciona con los elementos externos como la impresora, el ratón (o mouse), el teclado, el monitor y los demás periféricos (Cedano, Cedano, Rubio, y Vega, 2014, p.42).

m) **Información:** Vamos a utilizar el término información de una manera muy amplia. Fundamentalmente, entenderemos como tal cualquier cosa que pueda ser digitalizada codificada como un conjunto de bits. Para nuestro propósito, los resultados del fútbol, los libros, las bases de datos, las revistas, las películas, la música, los índices bursátiles y las páginas Web, son ejemplos de bienes de información. Donde centraremos en el valor que la información tiene para diferentes consumidores. La información puede tener valor como entretenimiento, y puede tener valor comercial, pero independientemente de cuál sea su valor, la gente está dispuesta a pagar por ella. Como veremos, muchas de las estrategias de los vendedores de información se basan en el hecho de que los consumidores valoran de formas muy distinta unos mismos bienes de información.

Por supuesto, la información es cara de crear y de ensamblar. La estructura de costes de un proveedor de información es bastante

peculiar estructura de costes, por ahí es por donde vamos a empezar a analizar la estrategia de la información. (Chapiro y Varian, 1999, p.2).

n) **Inventario:** El inventario de activos es la relación de todos aquellos elementos indispensables para el funcionamiento de la organización, ya que dan soporte a los procesos de negocio. Cuando se mencionó la estrategia para la definición del alcance del SGSI, se recomendaba la selección de servicios de negocio o servicios internos. Una buena manera de identificar activos es estudiar el funcionamiento de estos servicios planteando preguntas como: ¿Qué información es necesaria para prestar el servicio?, ¿Con qué aplicaciones se está gestionando esa información?, ¿Dónde se almacenan la información y las aplicaciones?, ¿Se han subcontratado servicios o productos de los que dependan?, ¿Por qué medios se transmite la información?, ¿De qué personas depende el servicio? (Gómez y Fernández, 2014, p.59).

o) **MAGERIT:** Es la metodología de análisis y gestión de riesgos desarrollada por el Consejo Superior de Administración Electrónica. Es un método formal adoptado por las Administraciones Públicas para investigar los riesgos que soportan los sistemas de información y recomendar las medidas adecuadas que deberán adoptarse para poder controlar dichos riesgos (Escrivá, 2013, p.8).

p) **Mantenimiento:** En esta fase se realizarán correcciones al sistema desarrollado, ya sea para solventar errores no depurados, o para cambiar o añadir nuevas funcionalidades requeridas por el cliente. Dependiendo de la importancia del caso, será necesario retomar el ciclo de vida a nivel de codificación, diseño o incluso análisis. Cuanto mejor se haya documentado el desarrollo en las primeras fases del ciclo de vida, menor será el tiempo necesario para llevar a cabo los distintos tipos de mantenimiento (Cedano, 2014, p.163).

q) **Monitorización:** No basta con diseñar e implantar una red informática en una organización, es necesario monitorizar y evaluar el rendimiento de la misma a lo largo de su vida mediante herramientas que permitan conocer cómo se comporta y si se está haciendo un uso indebido que ocasione un consumo excesivo del ancho de banda (Escrivá, 2013, p.179).

r) **Pilar:** Es una aplicación implementada por la metodología MAGERIT, para el análisis y gestión de riesgos de un sistema de información. Ha sido desarrollada por el Centro Criptológico Nacional (CCN) y es de amplia utilización en la Administración Pública española (Escrivá, 2013, p,12).

s) **Planificación:** Hay que invertir tiempo en hacerla, puesto que las decisiones y acciones que provoca afectan durante mucho tiempo (Colobran, Arqués y Marco, 2008, p.14).

t) **Política:** Es la información documentada en la que se reflejan, en términos generales, los objetivos de la organización en materia de seguridad de la información y las principales líneas de acción que permitan proteger su información frente a pérdidas de confidencialidad, integridad y disponibilidad. Tendrá en cuenta los requisitos del negocio, así como los contractuales, legales y estatutarios, los cuales quedarán reflejados en la misma.

   En la política de seguridad de la información, la organización adquiere el compromiso de implantar y mejorar de manera continua el sistema de gestión. Se trata de un documento que debe ser comunicado a todos los empleados y a otras partes interesadas: proveedores, clientes, usuarios, etc. (Gómez y Fernández, 2014, p.20).

u) **Procedimientos:** Es uno de los puntos más problemáticos. El objetivo de un procedimiento es describir la manera en la que se va a realizar una tarea. El nivel de detalle de un procedimiento no

debería ser muy alto. Se trata de contar cómo se hace una tarea de forma que alguien que no esté familiarizado con ella pudiera ejecutarla en caso necesario. Para ello se debería describir a grandes rasgos lo que se debe hacer y citar aquellos documentos que puedan ser de ayuda para llevar a cabo la tarea. Se debe evitar ofrecer detalles que pueden cambiar con frecuencia, y obligarían a revisar el procedimiento muy a menudo. Este tipo de datos deberían documentarse en instrucciones técnicas y no en procedimientos (Gómez y Álvarez, 2012, p.86).

v) **Red:** Una red de ordenadores es un conjunto de ordenadores autónomos interconectados entre sí. Dos ordenadores están conectados entre sí cuando pueden intercambiar información y son autónomos cuando no existe una relación maestro/esclavo entre ellos. La comunicación entres hosts dentro de una red de ordenadores es un proceso de alto grado de complejidad, de manera que la mayor parte de las redes se han diseñado separando su organización en varias capas (Aznar, 2004, p.15).

w) **Riesgo:** En términos generales, el riesgo se define como la posibilidad de que no se obtengan los resultados deseados. En informática, las empresas nunca desean sufrir un ataque externo o interno a sus sistemas de información, pero los ataques siempre suceden, de manera que esa posibilidad o probabilidad se materializa. La empresa siempre está amenazada de sufrir algún daño en su sistema informático, daño que puede provocar pérdidas de muchos tipos, y las amenazas son mayores cuando los sistemas de información presentan ciertos puntos débiles llamados “vulnerabilidades”, de manera que se tiene mayor o menor riesgo dependiendo de la cantidad y número de vulnerabilidades que se tengan (Baca, 2016, p.23).

x) **Roles:** El acceso a la información también puede controlarse a través de la función, perfil o rol del usuario que requiere dicho

acceso. Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc. En este caso los derechos de acceso y políticas de seguridad asociadas pueden agruparse de acuerdo con el rol de los usuarios (Costas, 2006, p.93).

y) **Salvaguardas:** Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otras seguridades físicas y, por último, está la política de personal (Dirección General de Modernización Administrativa Libro I - Método, 2012, p.31)

z) **Seguridad:** La información está dentro la red de la organización, en servidores, en estaciones de trabajo, portátiles, etc. El personal accede, y es con los mecanismos de accesos que se limita y se controla quién puede acceder a esta información, de qué manera y qué puede hacer. Un diseño del entorno de usuarios correcto es el primer paso para evitar accesos no deseados a la información. El otro paso para tener sistemas seguros es evitar intrusiones. Es muy difícil tener sistemas completamente seguros, por lo tanto, sólo podemos intentar hacer el sistema tan seguro como sea posible (Colobran, 2008, p.170).

aa) **SGSI:** Debido a la complejidad de llevar a cabo un plan de seguridad, es necesaria una metodología. Por este motivo aparecieron los sistemas de gestión de la seguridad de la información (SGSI) En general, cualquier sistema de gestión de la seguridad, tendrá que comprender la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la Gestión de la Seguridad de la información dentro de una organización (Colobran, 2008, p.272).

bb) Sistema de Información: Podemos plantear la definición técnica de un sistema de información como un conjunto de componentes interrelacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar los procesos de toma de decisiones y de control en una organización. Además de apoyar la toma de decisiones, la coordinación y el control, los sistemas de información también pueden ayudar a los gerentes y trabajadores del conocimiento a analizar problemas, visualizar temas complejos y crear nuevos productos (Laudon y Laudon, 2012, p.15).

cc) Software: programas o aplicaciones que utiliza la organización para su buen funcionamiento o para automatizar los procesos de su negocio. Entre estos se pueden encontrar las aplicaciones comerciales, los sistemas operativos, etc. (Escrivá, 2013, p.8).

dd) Vulnerabilidad: En el campo de la seguridad informática se considera como vulnerabilidad a cualquier debilidad de un activo que pueda repercutir de alguna forma sobre el correcto funcionamiento del sistema informático. Estas debilidades, también conocidas como “agujeros de seguridad”, pueden estar asociadas a fallos en la implementación de las aplicaciones o en la configuración del sistema operativo, a descuidos en la utilización de los sistemas, etc. Por ejemplo, no utilizar ningún tipo de protección frente a fallos eléctricos o carecer de mecanismos de protección frente a ataques informáticos, como antivirus o cortafuegos (Escrivá, 2013, p.8).

III. MARCO METODOLÓGICO

3.1. Hipótesis de la Investigación

3.1.1. Hipótesis general

La propuesta de un Sistema de Gestión de Seguridad de la Información es adecuada para el Proyecto Especial Camélidos Sudamericanos (PECSA) del Gobierno Regional Puno; Aplicando la Metodología Magerit, influirá de forma positiva

3.2. Variables de Estudio

3.2.1. Definición conceptual

Sistema de Gestión de Seguridad de la Información.

3.2.2. Definición operacional

a) Sistema de Gestión de Seguridad de la Información

Un Sistemas de Gestión comprende todo lo concerniente a la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar El Sistema de Gestión de la Seguridad de la Información.

Según la **Dirección General de Modernización Administrativa - Libro I, (2012)** Se define “Sistema de Gestión” como lo que la Organización hace para gestionar sus procesos o actividades, de forma que los productos que fabrica o los servicios que presta satisfagan los objetivos que la propia organización de ha marcado,

típicamente.

- ✓ Satisfacer la calidad demandada por los clientes
- ✓ Cumplir con las obligaciones legales, regulatorias y contractuales

Dentro del sistema de gestión de una Organización, se entiende por “sistema de gestión de la seguridad de la información” (SGSI) la parte relacionada con la seguridad de la información. Es habitual entender que los Sistemas de Gestión deben ajustarse al llamado ciclo de **Denning (PDCA)**, habitual en Sistemas de Gestión de la Calidad:

P – Plan – Se establecen objetivos y se preparan planes para alcanzarlos. Esto incluye analizar la situación de la Organización: dónde estamos y dónde queremos estar.

D – Do – Se ejecutan los planes.

C – Check – Se evalúan los resultados obtenidos para determinar en qué medida se han alcanzado los objetivos propuestos.

A – Act – A fin de estar cada día mejor (mejora continua), se actualizan los planes y su implantación.

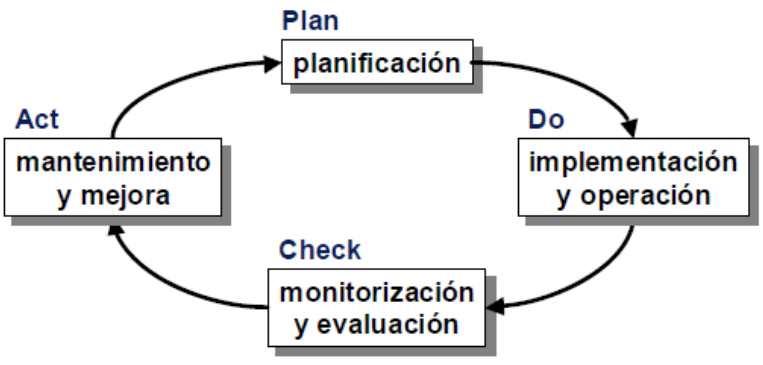


Figura 4: Ciclo PDCA
Fuente: Libro I – Método (2012)

La planificación (P de Plan) debe incluir una política de seguridad que marque objetivos y un análisis de riesgos que modele el valor del sistema, su exposición a amenazas, y lo que se tiene (o se necesita) para mantener el riesgo bajo control. Es natural que con estas bases se genere un plan de seguridad razonado para la gestión de riesgos.

La acción (D de Do) es la ejecución del plan, en sus aspectos técnicos y de organización, involucrando a las personas que se hacen cargo del sistema o están relacionadas con éste. Un plan tiene éxito cuando lleva a una operación diaria sin sorpresas.

La monitorización (C de Check) de la operación del sistema parte del hecho de que no se puede confiar ciegamente en la eficacia de las medidas, sino que continuamente hay que evaluar si responden a lo esperado con la eficacia deseada. Hay que medir tanto lo que ocurre como lo que ocurriría si no se hubieran tomado medidas. A veces se habla del “coste de la inseguridad” como justificación de que el gasto de dinero y esfuerzo tiene fundamento. Y hay que atender a las novedades que se produzcan, tanto en cuanto a modificaciones del propio sistema de información, como a nuevas amenazas.

La reacción (A de Act) es saber derivar consecuencias de la experiencia, propia y de sistemas similares, repitiendo el ciclo PDCA.

La evaluación de un Sistema de Gestión de la Seguridad parte del supuesto de que el esquema anterior vertebra las actuaciones de la Organización en materia de seguridad, y

juzga la eficacia de los controles implantados para alcanzar asegurarnos de que se alcanzan los objetivos propuestos. Nótese que un sistema de gestión maduro debe estar documentado en todos sus aspectos. Es típico de organizaciones inmaduras que las actividades se realizan siguiendo normas y procedimientos que se sobreentienden o están en la cabeza de las personas. Sólo cuando todo figura por escrito podemos hablar de un Sistema de Gestión que puede ser objeto de una certificación.

3.2.3. Operacionalización de la Variable.

Tabla 1: **Operacionalización de la Variable**

Variable	Dimensiones	Indicadores
Sistema de Gestión de Seguridad de la Información	Organización de la seguridad de la información	Roles y responsabilidades para la seguridad de la información
	Seguridad de los recursos humanos	Selección del empleado
		Términos y condiciones del empleo
	Gestión de activos	Inventario de activos
	Control de acceso	Políticas de control de acceso
		Gestión de derechos de acceso privilegiados
	Seguridad física y ambiental	Control de ingreso físico
		Mantenimiento de equipos
	Seguridad de las operaciones	Respaldo de la información
		Restricciones sobre la instalación de software
	Seguridad de las comunicaciones	Controles de red
		Seguridad de Servicios de Red
	Cumplimiento	Protección de registros
		Cumplimiento de políticas y normas de seguridad

Fuente: Elaboración propia del autor

3.3. Nivel de la Investigación

La presente investigación tiene por objetivo implementar un Sistema de Gestión de Seguridad de Información, para así asegurar que se

tiene implementado todos los controles adecuados sobre la confidencialidad, integridad y disponibilidad de la información, para ello se está utilizando el **tipo de investigación Documental y Descriptiva**.

Según **Bernal Torres (2010) La Investigación Documental** consiste en un análisis de la información escrita sobre un determinado tema, con el propósito de establecer relaciones, diferencias, etapas, posturas o estado actual del conocimiento respecto al tema objeto de estudio.

Según **Niño Rojas (2011) La Investigación Descriptiva** su propósito es describir la realidad objeto de estudio, un aspecto de ella, sus partes, sus clases, sus categorías o las relaciones que se pueden establecer entre varios objetos, con el fin de esclarecer una verdad, corroborar un enunciado o comprobar una hipótesis. Se entiende como el acto de representar por medio de palabras las características de fenómenos, hechos, situaciones, cosas, personas y demás seres vivos, de tal manera que quien lea o interprete, los evoque en la mente.

La investigación se ajusta a los lineamientos de un estudio de **tipo Documental y Descriptiva**, con la implementación de un Sistema de Gestión de Seguridad de Información; para así asegurar la confidencialidad, integridad y disponibilidad de la información que mejorará al Proyecto Especial Camélidos Sudamericanos - PECSA.

3.4. Diseño de la investigación

El presente estudio es de **diseño no experimental**

Según **Hernández Sampieri (2014)** La investigación no experimental es sistemática y empírica en la que las variables

independientes no se manipulan porque ya han sucedido. Las inferencias sobre las relaciones entre variables se realizan sin intervención o influencia directa, y dichas relaciones se observan tal como se han dado en su contexto natural.

Es un estudio no experimental no se construye ninguna situación, sino que se observan situaciones ya existentes, no provocadas intencionalmente por el investigador. En la investigación no experimental las variables independientes ya han ocurrido y no pueden ser manipuladas, el investigador no tiene control directo sobre dichas variables, no puede influir sobre ellas porque ya sucedieron, al igual que sus efectos.

3.5. Población y Muestra de Estudio

3.5.1. Población

Según **Hernández Sampieri (2014)** Una deficiencia que se presenta en algunos trabajos de investigación es que no describen lo suficiente las características de la población o consideran que la muestra la representa de manera automática. Suele ocurrir que algunos estudios que sólo se basan en muestras de estudiantes universitarios (porque es fácil aplicar en ellos el instrumento de medición, pues están a la mano) hagan generalizaciones temerarias sobre jóvenes que tal vez posean otras características sociales. Es preferible, entonces, establecer con claridad las características de la población, con la finalidad de delimitar cuáles serán los parámetros muestrales.

Es por ello que en esta investigación se trabajó con la técnica de la entrevista debido a la necesidad de obtener información directamente de la persona involucrada en el proceso o de

quien presenta la necesidad de la propuesta de investigación que es para el Proyecto Especial Camélidos Sudamericanos - PECSA ubicado en el Jr. Carabaya N°. 351 Puno – Puno, entidad que pertenece al Gobierno Regional Puno. Y su objetivo central está orientado a “Mejorar en Desarrollo de la Cadena de Valor de la fibra de Alpaca en la región Puno”, los sujetos informantes son el Director Ejecutivo y el Residente del Proyecto ya que es el encargado de centralizar toda la información que general el PECSA.

3.6. Técnicas e instrumentos de recolección de datos

3.6.1. Validez del Instrumento

Tabla 2: **Validación de expertos**

Dra. Wilver Auccahuasi Aiquipa	Experto temático
Mgtr. Edmundo Barrantes Ríos	Experto Metodólogo
Dra. Madeleine Bernardo Santiago	Experto Metodólogo

Fuente: Elaboración Propia del autor

3.6.2. Técnicas de recolección de datos

Según **G. Arias (2012)** Las técnicas de recolección de datos son las distintas formas o maneras de obtener la información. Son ejemplos de técnicas; la observación directa, la encuesta en sus dos modalidades: oral o escrita (cuestionario), la entrevista, el análisis documental, análisis de contenido, etc.

Los instrumentos son los medios materiales que se emplean para recoger y almacenar la información. Ejemplo: fichas, formatos de cuestionario, guía de entrevista, lista de cotejo, escalas de actitudes u opinión, grabador, cámara fotográfica o de video, etc.

En la presente investigación la técnica a usar será la

entrevista, debido a que este método de investigación permitirá recolectar información primaria y de primera fuente la cual consta de 25 ítems de preguntas cerradas a todo el personal involucrado del PECSA.

3.6.3. Instrumentos de recolección de datos

Para la presente investigación se utilizará la técnica de la encuesta y como instrumento la entrevista y según **Niño (2011)** Entendemos por encuesta la técnica que permite la recolección de datos que proporcionan los individuos de una población, o más comúnmente de una muestra de ella, para identificar sus opiniones, apreciaciones, puntos de vista, actitudes, intereses o experiencias, entre otros aspectos, mediante la aplicación de cuestionarios, técnicamente diseñados para tal fin. En nuestros días, se ha convertido en el procedimiento más utilizado en las investigaciones de corte social y educativo, y también en los estudios empresariales, de mercadeo y en los sondeos de carácter político.

3.7. Métodos de análisis de datos

En base a los datos obtenidos de la encuesta; se desarrollará la implementación del Sistema de Gestión de Seguridad de Información, aplicando la metodología de MAGERIT Versión 3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, en el que contribuirá a que la institución posea un conocimiento claro sobre los riesgos que pueden presentarse en sus sistemas de información.

Las fases que contempla el modelo MAGERIT Versión 3 son:

- ✓ **Planificación del Proyecto**: Establece el marco general de referencia para el proyecto.
- ✓ **Análisis de Riesgos:** Permite determinar cómo es, cuánto vale y cómo de protegidos se encuentran los activos.
- ✓ **Gestión de Riesgos:** Permite la selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

3.8. Aspectos éticos

Como profesional en servicio a la sociedad y a mi país prima en mí la honestidad para considerar los derechos de autor que se tipifican en esta investigación. En el rubro de tecnologías y seguridad de la información siguiendo lineamientos, metodologías y procesos de implementación que ayude al desarrollo. Es por esta razón que se siguieron las normas éticas al realizar esta investigación no experimental bajo las directrices en cuanto a normas para la elaboración de esta investigación.

IV. RESULTADOS

4.1. Resultados

4.1.1. Sistema de Gestión de Seguridad de la Información

La presente tesis está referida al siguiente título: “Propuesta de un Sistema de Gestión de Seguridad de la Información, Aplicando la Metodología Magerit Para el Gobierno Regional Puno”, Caso: Proyecto Especial Camélidos Sudamericanos – PECSA, 2017.

El Sistema de Gestión es la estructura organizada, la planificación de las actividades, las responsabilidades, las prácticas, todo aquel procedimiento, los procesos y los recursos para desarrollar, implantar, llevar a cabo revisar y mantener al día la política de la empresa. En otras palabras, es un método sistemático de control de las actividades, procesos y asuntos relevantes para una organización, que posibilite alcanzar los objetivos previstos y obtener el resultado deseado, a través de la participación e implicación de todos los miembros de la organización y garantizando la satisfacción del cliente, de la sociedad en general y de cualquier parte interesada.

4.1.2. Componentes del Sistema de Gestión

La presente tesis tiene como componente principal, realizar la implementación del Sistema de Gestión de Seguridad de la Información. Donde llegaremos principalmente para controlar el activo principal que es la información del Proyecto Especial Camélidos Sudamericanos – PECSA.

4.1.3. Objetivo del Sistema de Gestión

El Proyecto Especial Camélidos Sudamericanos – PECSA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

4.1.4. Alcance del Sistema de Gestión

El presente alcance aplica a toda la entidad, funcionarios, contratistas y terceros del Proyecto Especial Camélidos Sudamericanos – PECSA de la Región Puno.

4.1.5. Restricciones del Sistema de Gestión

Las restricciones de la presente Tesis fueron:

- ✓ En la investigación la principal restricción fue el acceso a la información del proyecto ya que constantemente realizan cambios de personal.
- ✓ También la limitación de validez de los resultados obtenidos en la investigación, son solamente de validez para el Proyecto Especial Camélidos Sudamericanos – PECSA.
- ✓ Toda investigación tiene restricciones solo a sistemas de información.

4.1.6. Estudio de Factibilidad del Sistema de Gestión

Al realizar el estudio de factibilidad para poder determinar la viabilidad de la implementación de un Sistema de Gestión de

Seguridad de la Información para el Proyecto Especial Camélidos Sudamericanos - PECSA, comprende la disponibilidad de los recursos necesarios para llevar a cabo los objetivos o metas señalados, el estudio de la factibilidad comprende 3 aspectos necesarios que son: Factibilidad Operativa, Factibilidad Técnica y Factibilidad Económica.

4.1.6.1. Factibilidad Operativa

En este puno se refiere a todo aquel recurso que interviene en algún tipo de actividades o procesos, dependiendo de los recursos humanos que participen durante la operación del proyecto, durante esta etapa se identifican todos los componentes y actividades que son necesarias para lograr el objetivo que se evalúa y donde se determinará todo lo necesario para llevarlo a cabo, siguiendo estos pasos:

a. Establecer el compromiso y el reconocimiento de la Dirección sobre las responsabilidades de seguridad de la información.

b. Verificar si existe el presupuesto necesario para capacitación del personal involucrado en el Diseño de un Sistema de Gestión de Seguridad de la Información para el Proyecto Especial Camélidos Sudamericanos - PECSA.

c. Establecer el compromiso necesario de la Dirección para el establecimiento de la Implementación del Sistema de Gestión de Seguridad de la Información para el Proyecto Especial Camélidos Sudamericanos – PECSA.

d. Realizar la implementación sobre los procedimientos básicos de Seguridad de Información y Políticas de Seguridad para el Proyecto Especial Camélidos Sudamericanos – PECSA.

Una vez realizado las actividades anteriores en el Proyecto Especial Camélidos Sudamericanos – PECSA, se determinará la Factibilidad Operativa, si los personales están en la mejor disposición y compromiso para Implementar un Sistema de Gestión de Seguridad de la Información.

4.1.6.2. Factibilidad Técnica

En este parte se refiere claramente al análisis de la política y controles que se requerirá para conseguir la funcionalidad y el rendimiento de la propuesta, cuál es el riesgo de desarrollo y cómo afectan estos elementos en el costo del proyecto. Además, se debe definir si el problema se puede resolver con los medios actualmente existentes y el grado de adaptación de la solución a la tecnología con la que cuenta el proyecto, para lo cual seguiremos los siguientes pasos:

a. Realizar el diagnóstico de las capacidades técnicas requeridas para las alternativas de implementación.

b. Verificar si el personal posee experiencia técnica para establecer la propuesta de un Sistema de Gestión de Seguridad de la Información.

c. Verificar que el personal con experiencia suficiente en el área de seguridad de la información que será

la encargada de supervisar la propuesta de un Sistema de Gestión de Seguridad de la Información para el Proyecto Especial Camélidos Sudamericanos - PECSA.

d. Evaluar la Infraestructura Tecnológica que posee la institución y las requeridas para la propuesta.

e. Analizar el grado de aceptación que genera la propuesta de un Sistema de Gestión de Seguridad de la Información para el Proyecto Especial Camélidos Sudamericanos.

Una vez realizado las actividades anteriores en el Proyecto Especial Camélidos Sudamericanos – PECSA se llegará a determinará la Factibilidad Técnica, si el personal que trabaja en el Proyecto tiene la experiencia técnica necesaria para la implementación y la Infraestructura Tecnológica que posee sean adecuadas para el proyecto.

4.1.6.3. Factibilidad Económica

En este punto daremos un análisis para determinar el costo beneficio para implementar un Sistema de Gestión de Seguridad de la Información para para el Proyecto Especial Camélidos Sudamericanos. Como también presentaremos un estudio que dio como resultado la factibilidad económica del desarrollo para la implementación del Sistema de Gestión de Seguridad de la Información. Determinaremos los recursos para desarrollar, implantar, y mantener en operación el Sistema de Gestión de Seguridad de la

Información programado, haciendo una evaluación donde se puso de manifiesto el equilibrio existente entre los costos específicos del SGSI y los beneficios que se derivaron de éste, lo cual permitió observar de una manera más precisa las bondades del sistema propuesto.

Económicamente el Sistema de Gestión de Seguridad de la Información implica una demanda de gasto debido a que se requiere personal especializado para realizar las capacitaciones, entrenamientos y auditorías internas para el buen manejo de Sistema de Gestión de Seguridad de la Información.

También se requerirá inversión en la adquisición de accesorios de tipo informático para el buen funcionamiento del SGSI.

4.1.7. Metodología Aplicada

4.1.7.1. Descripción de la Metodología aplicada

Según Gutierrez Amaya (2013) indica que MAGERIT es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados. Además de esto, cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos.

Puntualmente MAGERIT se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.

Lo interesante de esta metodología, es que presenta una guía completa y paso a paso de cómo llevar a cabo el análisis de riesgos. Esta metodología está dividida en tres libros. El primero de ellos hace referencia al **Libro I** – El Método, donde se describe la estructura que debe tener el modelo de gestión de riesgos. Este libro está de acuerdo a lo que propone ISO para la gestión de riesgos.

El **Libro II** es un Catálogo de Elementos, el cual es una especie de inventario que puede utilizar la empresa para enfocar el análisis de riesgo. Es así como contiene una división de los activos de información que deben considerarse, las características que deben tenerse en cuenta para valorar los activos identificados y además un listado con las amenazas y controles que deben tenerse en cuenta.

Finalmente, el **Libro III** es una Guía de Técnicas, lo cual lo convierte en un factor diferenciador con respecto a otras metodologías. En esta tercera parte se describen diferentes técnicas frecuentemente utilizadas en el análisis de riesgos. Contiene ejemplos de análisis con tablas, algoritmos, árboles de ataque, análisis de costo beneficio, técnicas gráficas y buenas prácticas para llevar adelante sesiones de trabajo para el análisis

de los riesgos.

Esta metodología es muy útil para aquellas empresas que inicien con la gestión de la seguridad de la información, pues permite enfocar los esfuerzos en los riesgos que pueden resultar más críticos para una empresa, es decir aquellos relacionados con los sistemas de información. Lo interesante es que al estar alineado con los estándares de ISO es que su implementación se convierte en el punto de partida para una certificación o para mejorar los sistemas de gestión.

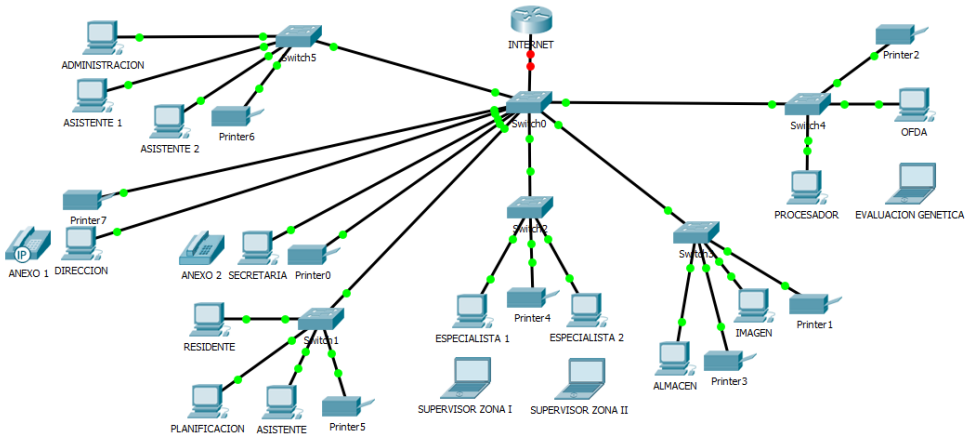


Figura 5: Diagrama de terminales
Fuente: Elaboración propia del autor

4.1.7.2. Fases /Etapas / Normas de la Metodología aplicada

a. Diagnóstico de la Situación Actual del PECSA.

Según la técnica de la entrevista se realizó a través de una lista de preguntas donde los resultados obtenidos serán necesarios para elaborar el presente trabajo de investigación.

b. Análisis de Riesgos

Los criterios a realizar son:

b.1. Determinación de Activos: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Teniéndose activos como:

- ✓ Datos que materializan la información
- ✓ Servicios auxiliares que se necesitan para poder organizar el sistema.
- ✓ Las aplicaciones informáticas (software) que permiten manejas los datos.
- ✓ Los equipos informáticos (hardware) y que permitan hospedar datos, aplicaciones y servicios.
- ✓ Los soportes de información que son dispositivos de almacenamiento d datos.
- ✓ El equipamiento auxiliar que complementa el material informático.
- ✓ Las redes de comunicaciones que permitan intercambiar datos.
- ✓ Las instalaciones que acogen equipos informáticos y de comunicaciones.
- ✓ Las personas que explotan u operan todos los elementos anteriormente citados.

No todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y salvaguardas son diferentes.

b.2. Caracterización de las Dimensiones del Activo: De un activo puede interesar calibrar diferentes dimensiones:

- ✓ Su **confidencialidad:** ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.

- ✓ Su **integridad:** ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcial-mente falsos o, incluso, faltar datos.

- ✓ Su **disponibilidad:** ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.

- ✓ La **autenticidad:** ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

  Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar)

- ✓ **La trazabilidad** del uso del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y

cuándo?

- ✓ **La trazabilidad** del acceso a los datos: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

b.3. Valoración de los Activos: La valoración se puede ver desde la perspectiva de la 'necesidad de proteger' pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes. El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un es-quema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

El valor nuclear suele estar en la información que el sistema maneja y los servicios que se prestan (activos denominados esenciales), quedando los demás activos subordinados a las necesidades de explotación y protección de lo esencial.

- ✓ Estimación del impacto Se puede calcular el impacto en base a tablas sencillas de doble entrada:

impacto		degradación		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Figura 6: Estimación del impacto
Fuente: Libro III – Guía de Técnicas, (2012)

Aquellos activos que reciban una calificación de impacto muy alto (MA) deberían ser objeto de atención inmediata.

- ✓ Estimación del riesgo: Por otra parte, se modelan impacto, probabilidad y riesgo por medio de escalas cualitativas:

escalas		
impacto	probabilidad	riesgo
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Figura 7: Estimación del Riesgo
Fuente: Libro III – Guía de Técnicas, (2012)

Pudiendo combinarse impacto y frecuencia en una tabla para calcular el riesgo:

riesgo		probabilidad				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Figura 8: Estimación del Riesgo
Fuente: Libro III – Guía de Técnicas, (2012)

b.4. Determinación de Amenazas: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

- ✓ De origen natural

  Hay accidentes naturales (terremotos, inundaciones, ...). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.

- ✓ Del entorno (de origen industrial)

  Hay desastres industriales (contaminación, fallos eléctricos, ...) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.

- ✓ Defectos de las aplicaciones

  Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se

denominan vulnerabilidades técnicas o, simplemente, ‘vulnerabilidades’13.

- ✓ Causadas por las personas de forma accidental las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

- ✓ Causadas por las personas de forma deliberada.

  Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

  No todas las amenazas afectan a todos los activos14, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

b.5. Salvaguardas: Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otra seguridad física y, por último, está la política de personal.

4.1.7.3. Modelamiento actual del proceso

Situación Actual del PECSA

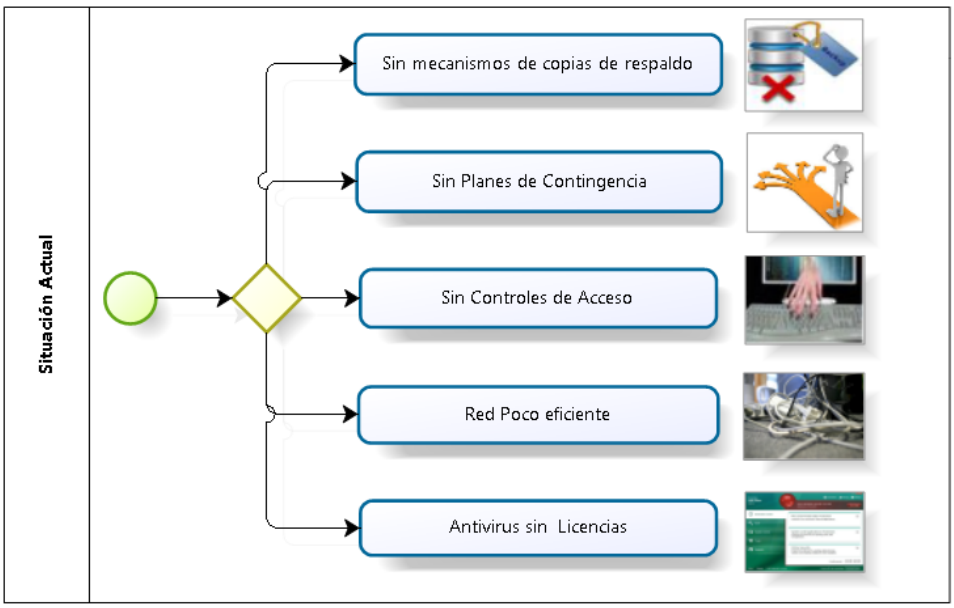


Figura 9: Situación Actual del PECSA
Fuente: Elaboración propia del autor

4.1.8. Propuesta del Sistema de Gestión de Seguridad de la Información.

4.1.8.1. Manuales del SGSI

Después de a ver analizado en el Proyecto Especial Camélidos Sudamericanos con la Metodología Magerit se ha identificado los riesgos más críticos y por los cuales se realiza un manual PECSA-M-01 que se encuentra en el Anexo.

4.1.8.2. Plan de acción

a. Elaborar la encuesta
b. Aplicación de la encuesta
c. Procesamiento de la encuesta
d. Determinación de la ejecución del método Magerit
e. Aplicación del método Magerit
f. Propuesta de SGSI

V. DISCUSIÓN

5.1. Análisis y Discusión de Resultados

Se desarrollaron las etapas de la metodología de análisis de información, a través de la aplicación de una investigación de campo al personal que labora en el PECSA.

a. Diagnóstico de la situación actual del Proyecto Especial Camélidos Sudamericanos.

En esta fase se realizó el análisis general de la situación actual de la Seguridad de la Información en el Proyecto Especial Camélidos Sudamericanos, basándonos en información recopilada mediante entrevista al Director Ejecutivo y al Residente del Proyecto Especial Camélidos Sudamericanos.

a.1. Organización de la seguridad de la información

Interpretación:

Según los resultados de la entrevista, aún no se tiene establecido los roles y responsabilidades frente al sistema de gestión de seguridad de la información y como también el representante de la alta dirección no tiene claro la importancia del control de la seguridad de la información.

a.2. Seguridad de los recursos humanos

Interpretación:

Según los resultados de la entrevista, no se tiene establecido un proceso disciplinario formal frente a las infracciones

cometidas por los empleados. Así mismo se evidencio que los empleados al finalizar su contrato no dejan su información digital, sin embargo, se cuenta con documentación física, sin la clasificación adecuada.

a.3. Gestión de Activos.

Interpretación

En el PECSA según los resultados de la entrevista, se cuenta con una identificación parcial de los activos de la institución; así también no se tiene una clasificación pertinente de la información.

a.4. Control de Acceso.

Interpretación:

Según los resultados de la entrevista, la información se encuentra accesible para cualquier usuario que pertenezca a la institución; ya que la institución no cuenta con un Servidor de Directorio Activo para que puedan actualizar o cambiar sus contraseñas.

a.5. Seguridad física y ambiental.

Interpretación:

En el PECSA según los datos obtenidos de la entrevista, no se cuenta con protecciones contra amenazas externas y ambientales como, por ejemplo: Mapa de evacuación, Extintores y señalizaciones de zona segura. Con respecto al mantenimiento preventivo de los equipos informáticos, se realiza de forma no planificada.

a.6. Seguridad de las operaciones.

Interpretación:

Según los datos recopilados de la entrevista no se tiene establecido una frecuencia para realizar copias de respaldo de la información del personal; por lo que esta actividad se realiza en función del requerimiento del usuario. Con respecto a los controles y restricciones para instalar software se cuenta con un mínimo porcentaje de restricción, debido que algún software es son necesarios para ejecutar el trabajo que tiene encargado cada usuario.

a.7. Seguridad de las comunicaciones.

Interpretación:

Según las entrevistas no se tiene un control adecuando de la red de datos, debido a que todo el personal puede acceder a cualquier tipo de página web que no tiene ninguna relación con las actividades de trabajo cotidianas.

a.8. Cumplimiento.

Interpretación:

Según el resultado de la entrevista; indican que se tiene parcialmente protegida la información con la instalación y actualización de antivirus. Con referente a la revisión del cumplimiento de la política, procedimientos y normas de la información por parte del director, esta no se realiza debido que no se tiene establecido este tipo de documentación.

b. Análisis de Riesgos

Una vez identificada la necesidad en la fase de diagnóstico, donde se determinó desarrollar una propuesta de Sistema de Gestión de Seguridad de la Información para PECSA, se procedió al establecimiento del Diseño del SGSI (Manual de SGSI: PECSA-M-01).

✓ Determinación de Activos:

Mediante reuniones y entrevistas al personal de PECSA se procedió con la identificación de los activos en dicha organización. Tal como se detalla en la siguiente tabla.

ACTIVOS		Tangible	Tipo de activo
APLICACIONES INFORMATICAS			
	Sistema Operativo	NO	Aplicación
	Microsoft Office	NO	Aplicación
	Diseñadores Gráficos	NO	Aplicación
	Software de Edición de Video y Audio	NO	Aplicación
	Antivirus	NO	Aplicación
	Correo Institucional	NO	Aplicación
	Página Web	NO	Aplicación
LAS INSTALACIONES			
	Computadoras de Escritorio y Laptop	SI	Tecnología
	OFDA 2000	SI	Tecnología
	Cámara Fotográfica	SI	Tecnología
	Filmadora	SI	Tecnología
	Teléfono	SI	Tecnología
	Impresora Multifuncional	SI	Tecnología
	Internet	SI	Tecnología
	Switch	SI	Tecnología
SOPORTES DE INFORMACIÓN			
	Memorias Externas	SI	Tecnología
DATOS			
	Documentos físicos	SI	Tecnología
PERSONAL			
	Personal Técnico	SI	Personal
	Personal Administrativo	SI	Personal
	Personal de Planificación	SI	Personal
	Personal de Residencia	SI	Personal
	Personal de Vigilancia	SI	Personal
LAS REDES DE COMUNICACIONES			
	Red Local	Si	Tecnologia

Figura 10: Determinación de Activos
Fuente: Elaboración Propia del autor

✓ Caracterización de las Dimensiones del Activo:

Basándonos en la metodología del Magerit se procede con la caracterización de las dimensiones de los activos.

ACTIVOS	DIMENSIONES DEL MAGERIT				
APLICACIONES INFORMATICAS	CONFIDENCIALIDAD	INTEGRADOR	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
Sistema Operativo					
Averia de origen físico o lógico	7	3	7		
Errores de los Usuario	7	3	5		
Errores del Administrador del Sistema	9	5	5		
Difusión de software dañino	3		5		
Errores de re-encaminamiento	3	5	3		
Destrucción de la Información	5	3	3		
Fuga de información	1		5		
Errores de mantenimiento / Actualizaciones de programas	3	3	3		
Microsoft Office					
Averia de origen físico o lógico	7	3	7		
Errores de los Usuario	7	3	5		
Errores del Administrador del Sistema	9	5	5		
Diseñadores Gráficos					
Averia de origen físico o lógico	7	3	7		
Vulnerabilidades de los programas	1		5		
Errores de mantenimiento / Actualizaciones de programas			7		
Software de Edición de Video y Audio					
Averia de origen físico o lógico	7	3	7		
Errores de los Usuario	7	3	5		
Errores de mantenimiento / Actualizaciones de programas			7		
Antivirus					
Errores de los Usuario	7	3	5		
Errores de mantenimiento / Actualizaciones de programas	3	5	3		
Correo Institucional					
Falta de renovación del servicio	7	3	7		
Caducidad del Servicio	7	3	5		
Mala configuración del Servicio	9	5	5		
Página Web					
Falta de renovación del servicio	7	3	7		
Caducidad del Servicio	7	3	5		
Mala configuración del Servicio	9	5	5		
LAS INSTALACIONES					
Computadoras de Escritorio y Laptop					
Errores de mantenimiento	3	3	5		
Incompatibilidad de los componentes		7	7		
Averia de origen físico o lógico	7	3	5		
Errores de los Usuario	7	3	3		
Difusión de software dañino	3		5		
OFDA 2000					
Errores de mantenimiento	3	3	5		
Incompatibilidad de los componentes		7	7		
Averia de origen físico o lógico	7	3	5		
Errores de los Usuario	7	3	3		
Difusión de software dañino	3		5		
Cámara Fotográfica					
Errores de los Usuario	7	3	3		
Filmadora					
Errores de los Usuario	7	3	3		
Teléfono					
Averia de origen físico o lógico	7	3	5		
Errores de los Usuario	7	3	3		
Impresora Multifuncional					
Averia de origen físico o lógico	7	3	7		
Errores de los Usuario	7	3	5		
Errores del Administrador del Sistema	9	5	5		
Internet					
Averia de origen físico o lógico	7	3	7		
Errores del Administrador del Sistema	9	5	5		
Switch					
Averia de origen físico o lógico	7	3	7		
Errores del Administrador del Sistema	9	5	5		
SOPORTES DE INFORMACIÓN					
Memorias Externas					
Averia de origen físico o lógico	7	3	5		
Errores de los Usuario	7	3	3		
DATOS					
Documentos físicos					
Errores de los Usuario	7	3	5	5	7
Fuga de información	1		5	7	5
PERSONAL					
Personal Técnico					
Fuga de información	3	5	5		
Daño voluntario	7	5	3		
Personal Administrativo					
Fuga de información	3	5	5		
Daño voluntario	7	5	3		
Personal de Planificación					
Fuga de información	3	5	5		
Daño voluntario	7	5	3		
Personal de Residencia					
Fuga de información	3	5	5		
Daño voluntario	7	5	3		
Personal de Vigilancia					
Fuga de información			5		
LAS REDES DE COMUNICACIONES					
Red Local					
Fallo de servicios de comunicaciones	7	3	7		
Errores del administrador del Sistema / de la seguridad	7	3	5		
Caída del sistema por agotamiento de recursos	9	5	5		
Uso no previsto	3		5		
Denegación de servicio	3	5	3		
Ataque destructivo	3	5	3		

Figura 11: Caracterización de las Dimensiones del Activo
Fuente: Elaboración Propia del autor

✓ Valoración de los Activos:

[pi] Información de carácter personal		
6	6.pi1	probablemente afecte gravemente a un grupo de individuos
	6.pi2	probablemente quebrante seriamente la ley o algún reglamento de protección de información personal

5	5.pi1	probablemente afecte gravemente a un individuo
	5.pi2	probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	probablemente afecte a un grupo de individuos
	4.pi2	probablemente quebrante leyes o regulaciones
3	3.pi1	probablemente afecte a un individuo
	3.pi2	probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	pudiera causar molestias a un individuo
	2.pi2	pudiera quebrantar de forma leve leyes o regulaciones
1	1.pi1	pudiera causar molestias a un individuo

[lpo] Obligaciones legales		
9	9.lro	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	probablemente sea causa de incumplimiento de una ley o regulación
3	3.lro	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1	1.lro	pudiera causar el incumplimiento leve o técnico de una ley o regulación

[si] Seguridad		
10	10.si	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	9.si	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	7.si	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	3.si	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1	1.si	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

[cei] Intereses comerciales o económicos		
9	9.cei.a	de enorme interés para la competencia
	9.cei.b	de muy elevado valor comercial
	9.cei.c	causa de pérdidas económicas excepcionalmente elevadas
	9.cei.d	causa de muy significativas ganancias o ventajas para individuos u organizaciones
	9.cei.e	constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7	7.cei.a	de alto interés para la competencia
	7.cei.b	de elevado valor comercial
	7.cei.c	causa de graves pérdidas económicas
	7.cei.d	proporciona ganancias o ventajas desmedidas a individuos u organizaciones

	7.cei.e	constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
3	3.cei.a	de cierto interés para la competencia
	3.cei.b	de cierto valor comercial
	3.cei.c	causa de pérdidas financieras o merma de ingresos
	3.cei.d	facilita ventajas desproporcionadas a individuos u organizaciones
	3.cei.e	constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei.a	de bajo interés para la competencia
	2.cei.b	de bajo valor comercial
1	1.cei.a	de pequeño interés para la competencia
	1.cei.b	de pequeño valor comercial
0	0.3	supondría pérdidas económicas mínimas

[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización

[po] Orden público		
9	9.po	alteración seria del orden público
6	6.po	probablemente cause manifestaciones, o presiones significativas
3	3.po	causa de protestas puntuales
1	1.po	pudiera causar protestas puntuales

[olm] Operaciones		
10	10.olm	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	9.olm	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7	7.olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5	5.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3	3.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1	1.olm	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)

[adm] Administración y gestión		
9	9.adm	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7	7.adm	probablemente impediría la operación efectiva de la Organización
5	5.adm	probablemente impediría la operación efectiva de más de una parte de la Organización
3	3.adm	probablemente impediría la operación efectiva de una parte de la Organización
1	1.adm	pudiera impedir la operación efectiva de una parte de la Organización

[lg] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	no supondría daño a la reputación o buena imagen de las personas u organizaciones

[crm] Persecución de delitos		
8	8.crm	Impida la investigación de delitos graves o facilite su comisión
4	4.crm	Dificulte la investigación o facilite la comisión de delitos

[rto] Tiempo de recuperación del servicio		
7	7.rto	RTO < 4 horas
4	4.rto	4 horas < RTO < 1 día
1	1.rto	1 día < RTO < 5 días
0	0.rto	5 días < RTO

[lbl.nat] Información clasificada (nacional)		
10	10.lbl	Secreto
9	9.lbl	Reservado
8	8.lbl	Confidencial
7	7.lbl	Confidencial
6	6.lbl	Difusión limitada
5	5.lbl	Difusión limitada
4	4.lbl	Difusión limitada
3	3.lbl	Difusión limitada
2	2.lbl	Sin clasificar
1	1.lbl	Sin clasificar

[lbl.ue] Información clasificada (Unión Europea)		
10	10.ue	TRES SECRET UE
9	9.ue	SECRET UE
8	8.ue	CONFIDENTIEL UE
7	7.ue	CONFIDENTIEL UE
6	6.ue	RESTREINT UE
5	5.ue	RESTREINT UE
4	4.ue	RESTREINT UE
3	3.ue	RESTREINT UE

Figura 12: Valoración de los activos
Fuente: Libro II – Catalogo de Elementos (2012)

✓ Determinación de Amenazas:

[N] Desastres naturales
- [N.1] Fuego
- [N.2] Daños por agua
- [N.*] Desastres naturales

[I] De origen industrial
- [I.1] Fuego
- [I.2] Daños por agua
- [I.*] Desastres industriales
- [I.3] Contaminación mecánica
- [I.4] Contaminación electromagnética
- [I.5] Avería de origen físico o lógico
- [I.6] Corte del suministro eléctrico
- [I.7] Condiciones inadecuadas de temperatura o humedad
- [I.8] Fallo de servicios de comunicaciones
- [I.9] Interrupción de otros servicios y suministros esenciales
- [I.10] Degradación de los soportes de almacenamiento de la información
- [I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados
- [E.1] Errores de los usuarios
- [E.2] Errores del administrador
- [E.3] Errores de monitorización *(log)*
- [E.4] Errores de configuración
- [E.7] Deficiencias en la organización
- [E.8] Difusión de software dañino
- [E.9] Errores de [re-]encaminamiento
- [E.10] Errores de secuencia
- [E.14] Escapes de información
- [E.15] Alteración accidental de la información
- [E.18] Destrucción de información
- [E.19] Fugas de información
- [E.20] Vulnerabilidades de los programas (software)
- [E.21] Errores de mantenimiento / actualización de programas (software)
- [E.23] Errores de mantenimiento / actualización de equipos (hardware)
- [E.24] Caída del sistema por agotamiento de recursos
- [E.25] Pérdida de equipos
- [E.28] Indisponibilidad del personal

[A] Ataques intencionados
- [A.3] Manipulación de los registros de actividad (log)
- [A.4] Manipulación de la configuración
- [A.5] Suplantación de la identidad del usuario
- [A.6] Abuso de privilegios de acceso
- [A.7] Uso no previsto
- [A.8] Difusión de software dañino
- [A.9] [Re-]encaminamiento de mensajes
- [A.10] Alteración de secuencia
- [A.11] Acceso no autorizado
- [A.12] Análisis de tráfico
- [A.13] Repudio
- [A.14] Interceptación de información (escucha)
- [A.15] Modificación deliberada de la información
- [A.18] Destrucción de información
- [A.19] Divulgación de información

[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)
Correlación de errores y ataques
Nuevas amenazas: XML
Sintaxis BNF
Esquema XSD
Nivel de la amenaza: XML
Sintaxis BNF
Esquema XSD
Referencias

Figura 13: Determinación de las Amenazas
Fuente: Libro II – Catálogo de Elementos

- ✓ Salvaguardas:

Protecciones generales u horizontales
Protección de los datos / información
Protección de las claves criptográficas
Protección de los servicios
Protección de las aplicaciones (software)
Protección de los equipos (hardware)
Protección de las comunicaciones
Protección en los puntos de interconexión con otros sistemas
Protección de los soportes de información
Protección de los elementos auxiliares
Seguridad física – Protección de las instalaciones
Salvaguardas relativas al personal
Salvaguardas de tipo organizativo
Continuidad de operaciones
Externalización
Adquisición y desarrollo
Referencias

Figura 14: Salvaguardas
Fuente: Libro II – Catálogo de Elementos

c. Gestión de Riesgos

Aplicando el método MAGERIT, se determinó los riesgos más críticos, del cual se va proceder a proponer el SGSI, mediante el manual del SGSI (PECSA-M-01), según los siguientes resultados:

ACTIVOS	DIMENSIONES DEL MAGERIT				
APLICACIONES INFORMATICAS	CONFIDENCIALIDAD	INTEGRADOR	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
Sistema Operativo					
Averia de origen físico o lógico	7	3	7		
Errores de los Usuario	7	3	5		
Errores del Administrador del Sistema	9	5	5		
Difusión de software dañino	3		5		
Errores de re-encaminamiento	3	5	3		
Destrucción de la Información	5	3	3		
Fuga de información	1		5		
Errores de mantenimiento / Actualizaciones de programas	3	3	3		
Microsoft Office					
Averia de origen físico o lógico	7	3	7		
Errores de los Usuario	7	3	5		
Errores del Administrador del Sistema	9	5	5		
Diseñadores Gráficos					
Averia de origen físico o lógico	7	3	7		
Vulnerabilidades de los programas	1		5		
Errores de mantenimiento / Actualizaciones de programas			7		
Software de Edición de Video y Audio					
Averia de origen físico o lógico	7	3	7		
Errores de los Usuario	7	3	5		
Errores de mantenimiento / Actualizaciones de programas			7		
Antivirus					
Errores de los Usuario	7	3	5		
Errores de mantenimiento / Actualizaciones de programas	3	5	3		
Correo Institucional					
Falta de renovación del servicio	7	3	7		
Caducidad del Servicio	7	3	5		
Mala configuración del Servicio	9	5	5		
Página Web					
Falta de renovación del servicio	7	3	7		
Caducidad del Servicio	7	3	5		
Mala configuración del Servicio	9	5	5		
LAS INSTALACIONES					
Computadoras de Escritorio y Laptop					
Errores de mantenimiento	3	3	5		
Incompatibilidad de los componentes		7	7		
Averia de origen físico o lógico	7	3	5		
Errores de los Usuario	7	3	3		
Difusión de software dañino	3		5		
OFDA 2000					
Errores de mantenimiento	3	3	5		
Incompatibilidad de los componentes		7	7		
Averia de origen físico o lógico	7	3	5		
Errores de los Usuario	7	3	3		
Difusión de software dañino	3		5		
Cámara Fotográfica					
Errores de los Usuario	7	3	3		
Cámara Fotográfica					
Errores de los Usuario	7	3	3		
Filmadora					
Errores de los Usuario	7	3	3		
Teléfono					
Averia de origen físico o lógico	7	3	5		
Errores de los Usuario	7	3	3		
Impresora Multifuncional					
Averia de origen físico o lógico	7	3	7		
Errores de los Usuario	7	3	5		
Errores del Administrador del Sistema	9	5	5		
Internet					
Averia de origen físico o lógico	7	3	7		
Errores del Administrador del Sistema	9	5	5		
Switch					
Averia de origen físico o lógico	7	3	7		
Errores del Administrador del Sistema	9	5	5		
SOPORTES DE INFORMACIÓN					
Memorias Externas					
Averia de origen físico o lógico	7	3	5		
Errores de los Usuario	7	3	3		
TOS					
Documentos físicos					
Errores de los Usuario	7	3	5	5	7
Fuga de información	1		5	7	5
PERSONAL					
Personal Técnico					
Fuga de información	3	5	5		
Daño voluntario	7	5	3		
Personal Administrativo					
Fuga de información	3	5	5		
Daño voluntario	7	5	3		
Personal de Planificación					
Fuga de información	3	5	5		
Daño voluntario	7	5	3		
Personal de Residencia					
Fuga de información	3	5	5		
Daño voluntario	7	5	3		
Personal de Vigilancia					
Fuga de información			5		
LAS REDES DE COMUNICACIONES					
Red Local					
Fallo de servicios de comunicaciones	7	3	7		
Errores del administrador del Sistema / de la seguridad	7	3	5		
Caída del sistema por agotamiento de recursos	9	5	5		
Uso no previsto	3		5		
Denegación de servicio	3	5	3		
Ataque destructivo	3	5	3		

Figura 15: Evaluación del nivel de criticidad de los riesgos
Fuente: Elaboración propia del autor

Interpretación: De acuerdo a los resultados obtenidos se propone una política y el Manual del Sistema de Gestión de Seguridad de la Información para PECSA en término de las características de su ubicación, activos y tecnología. (Anexo 4 y Anexo 5).

VI. CONCLUSIONES

6.1. Conclusiones

PRIMERA: Se realizó la propuesta de un Sistema de Gestión de Seguridad de la Información adecuada y pertinente, según los riesgos más críticos identificados con la metodología MAGERIT, con información de primera fuente del cual se elaboró un Manual del SGSI (PECSA-M-01), para el Caso: Proyecto Especial Camélidos Sudamericanos – PECSA, 2017, del Gobierno Regional Puno.

SEGUNDA: Del diagnóstico de la situación actual del PECSA, según el personal entrevistado, respondieron de forma negativa; evidenciando que el PECSA no cuenta con un Sistema de Gestión de Seguridad de la Información, por lo cual se procedió con la ejecución de la metodología del método MAGERIT.

TERCERA: Mediante el uso de la metodología MAGERIT, se procedió con la identificación de los Activos del PECSA, lo que permitió identificar los activos de aplicaciones informáticas, las instalaciones, soportes de información, datos, personal y las redes de comunicaciones.

CUARTA: Los controles del sistema de gestión de seguridad de la información, se hallaron en función del uso de la Herramienta PILAR, donde se determinaron los Activos de alta criticidad, como: D5: Seguridad Física y Ambiental; D8: Cumplimiento. En la Propuesta del Manual del SGSI (PECSA-M-01), ya se plasmó los controles pertinentes.

QUINTA: Se propone una Política y un Manual del SGSI para el Proyecto Especial Camélidos Sudamericanos – PECSA, dentro del cual se establecen los criterios para la implementación, control, seguimiento y mejora continua del SGSI.

VII. RECOMENDACIONES

7.1. Recomendaciones

PRIMERA: Se recomienda que la propuesta del SGSI (Manual del SGSI: PECSA-M-01) debe de implementarse en el proyecto especial de camélidos sudamericanos (PECSA) del Gobierno Regional Puno, a la brevedad posible.

SEGUNDA: Se debe de seguir cumpliendo con el diagnostico situacional, ahora llamado Auditorías Internas y Externas, propuesto en el Manual del SGSI (PECSA-M-01), como sistema de medición, que permita valorar la marcha del SGSI de modo global y particular.

TERCERA: Tal como se realizó el uso de la metodología MAGERIT, para la identificación de Activos del SGSI; se debe de continuar con la misma metodología para la mejora continua.

CUARTA: Se recomienda el uso de la Herramienta PILAR, para la valoración de los Activos de Alta Criticidad, en el cual te menciona las Salvaguardas que se implementaran para los controles del SGSI.

QUINTA: Poner en marcha la ejecución de la implementación de la Política y de Manual de SGSI, para evitar la pérdida de la información el Proyecto Especial Camélidos Sudamericanos (PECSA).

REFERENCIAS BIBLIOGRÁFICAS

Artículos

Adrés, A., y Gómez, L. (2009). Guía de aplicación de la Norma UNE-ISO / IEC 27001 sobre seguridad en sistemas de información para pymes. (AENOR, Ed.). España.

Camila Bolaños, M., y Rocha Galvis, M. (2014). Auditoría de Sistemas de Información. Retrieved from http://asijav.weebly.com/auditoria-de-sistemas-de-informacioacuten/magerit-v3-metodologa-de-anlisis-y-gestin-de-riesgos-de-los-sistemas-de-informacin

Libros

Aguilera López, P. (2010). *Seguridad Informatica* (1ra. Edici). Madrid: EDITEX.

Aguirre Mollehuanca, D. A. (2014). *DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA SERVICIOS POSTALES DEL PERÚ S.A.* PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ. Retrieved from http://tesis.pucp.edu.pe/repositorio/handle/123456789/5677

Areitio Bertolín, J. (2008). *Seguridad de la Información Redes, Informática y Sistemas de Información* (1ra Edició). Madrid: Ediciones Paraninfo S.A.

Arias, F. G. (2012). *El Proyecto de Investigación Introducción a la Metodología Científica* (6a Edición). Caracas - Venezuela: Editorial Episteme.

Arteaga Basurto, C., & Gonzáles Montaño, M. V. (2001). *Diagnóstico* (1ra. Edici). Mexico: UNAM.

Aznar López, A. (2004). *La red Internet. El modelo TCP/IP* (1ra. Edici). Grupo Abantos.

Baca Urbina, G. (2016). *Introducción a la Seguridad Informática* (1ra. Edici). Mexico: Grupo Editorial Patria. Retrieved from https://books.google.com.co/books?id=IhUhDgAAQBAJ&pg=PA12&lpg=PA12&dq=se+encarga+de+proteger+la+integridad+y+privacidad+de+la+información+almacenada+en+un+sistema+informático&source=bl&ots=0WKz9DvgIr&sig=A_3bwLDYhNvW_WqHSMRhyx4QQ1s&hl=es&sa=X&ved=0ahUKEwi

Bernal Torres, C. A. (2010). *Metodología de la Investigación* (3ra Edició).

Colombia: Worldcolor.

Camila Bolaños, M., & Rocha Galvis, M. (2014). Auditoría de Sistemas de Información. Retrieved from http://asijav.weebly.com/auditoria-de-sistemas-de-informacioacuten/magerit-v3-metodologa-de-anlisis-y-gestin-de-riesgos-de-los-sistemas-de-informacin

Cedano Olvera, M. A., Cedano Rodríguez, A., Rubio Gonzáles, J. A., & Vega Gutiérrez, A. C. (2014). *Fundamentos de Computación para Ingenieros* (1ra. Edici). Mexico: Grupo Editorial Patria.

Chapiro, C., & Varian, H. R. (1999). *El dominio de la Información.pdf* (1ra. Edici). España: INO Reproducciones, S.A.

Chicano Tejada, E. (2014). *Gestión de Incidentes de Seguridad Informática*. *proyecto AMPARO* (1ra. Edici, Vol. 3). España: IC Editorial. Retrieved from http://www.proyectoamparo.net/

Colobran Huguet, M., Arqués Soldevila, J. M., & Marco Galindo, E. (2008). *Administración de Sistemas Operativos en Red* (1ra. Edici). Barcelona: Editorial UOC.

Costas Santos, J. (2014). *Seguridad Informática* (1ra. Edici). Madrid: RA-MA S.A.

David, C. A. J., & Catalina, A. B. (2013). *DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL GRUPO EMPRESARIAL LA OFRENDA*. Universidad Tecnológica de Pereira. Retrieved from http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf?sequence=1

Dirección General de Modernización Administrativa, P. e I. de la A. E. (2012a). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I - Método* (Versión 3.). Madrid: Ministerio de Hacienda y Administraciones Públicas.

Dirección General de Modernización Administrativa, P. e I. de la A. E. (2012b). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro III - Guía de Técnicas* (Versión 3.). Madrid: Ministerio de Hacienda y Administraciones Públicas.

Escrivá Gascó, G. (2013). *Seguridad informática* (1ra. Edici). España: MACMILLAN Profesional.

Fernández García, R. (2006). *Sistema de Gestión de Calidad Ambiente y*

Prevención de Riesgos Laborales. Su Integración. (1ra. Edici). España: Imprenta Gamma.

García Paredes, A. (2016). *IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, APLICADO A LOS RIESGOS ASOCIADOS A LOS ACTIVOS DE INFORMACIÓN EN LA EMPRESA NET - CONSULTORES S.A.C*. UNIVERSIDAD NACIONAL DE SAN MARTÍN - T. Retrieved from http://tesis.unsm.edu.pe/xmlui/handle/11458/596

Gómez Fernández, L., & Andrés Álvarez, A. (2012). *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes* (2da. Edici). España: AENOR. Retrieved from http://www.academia.edu/download/36974512/NOV_DOC_Tabla_AEN_22994_1.pdf

Gómez Fernández, L., & Fernández Rivero, P. P. (2014). *Cómo implantar un SGSI según UNE-ISO / IEC 27001 : 2014 y su aplicación en el Esquema Nacional de Seguridad* (1ra. Edici). España: AENOR.

Guamán Seis, J. A. (2015). *Escuela politécnica nacional*. ESCUELA POLITÉCNICA NACIONAL. Retrieved from http://bibdigital.epn.edu.ec/bitstream/15000/10439/3/CD-6187.pdf

Gutierrez Amaya, C. (2013). MAGERIT: Metodología práctica para gestionar riesgos, 1–2. Retrieved from https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. del P. (2014). *METODOLOGÍA DE LA INVESTIGACIÓN* (6TA EDICIO). MEXICO: McGRAW-HILL/INTERAMERICANA EDITORES S.A. DE C.V.

Laudon, K. C., & Laudon, J. P. (2012). *Sistemas de Información Gerencial* (Decimosegu). México: PEARSON.

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro II - Catálogo de Elementos. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro II - Catálogo de Elementos* (Versión 3.). Madrid: Ministerio de Hacienda y Administraciones Publicas.

Niño Rojas, V. M. (2011). *Metodología de la Investigación Diseño y ejecución* (1ra. Edici). Bogotá, Colombia: Ediciones de la U.

NTP-ISO/IEC 27001:2014. (2014). NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE

LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. *Normas Técnicas Peruanas*, 45. Retrieved from http://www.pecert.gob.pe/_publicaciones/2014/ISO-IEC-27001-2014.pdf

Tola Franco, D. E. (2015). *Facultad de Ingeniería en Electricidad y Computación Presentado por :* Retrieved from https://www.dspace.espol.edu.ec/retrieve/89073/D-84631.pdf

Vasco Rodrigo, T. A. (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*. PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ.

Villena Aguilar, M. A. (2006). *SISTEMA DE GESTION DE SEGURIDAD DE INFORMACION PARA UNA INSTITUCION FINANCIERA*. *Test*. Pontificia Universidad Católica del Perú. https://doi.org/10.1017/CBO9781107415324.004

Tesis

Aguirre Mollehuanca, D. A. (2014). Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A. Pontificia Universidad Católica del Perú. Retrieved from http://tesis.pucp.edu.pe/repositorio/handle/123456789/5677

David, C. A. J., y Catalina, A. B. (2013). diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda. Universidad Tecnológica de Pereira. Retrieved from http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf?sequence=1

García Paredes, A. (2016). implementación de un sistema de gestión de seguridad de la información, aplicado a los riesgos asociados a los activos de información en la empresa net - consultores s.a.c. universidad nacional de san martín - T. Retrieved from http://tesis.unsm.edu.pe/xmlui/handle/11458/596

Guamán Seis, J. A. (2015). Facultad de Ingeniería de Sistemas Presentado por : Retrieved from http://bibdigital.epn.edu.ec/bitstream/15000/10439/3/CD-6187.pdf

Tola Franco, D. E. (2015). Facultad de Ingeniería en Electricidad y Computación

Presentado por : Retrieved from https://www.dspace.espol.edu.ec/retrieve/89073/D-84631.pdf

Villena Aguilar, M. A. (2006). Sistema de gestion de seguridad de informacion para una institucion financiera. Test. Pontificia Universidad Católica del Perú. https://doi.org/10.1017/CBO9781107415324.004

ANEXOS

ANEXO 1: Matriz de Consistencia

PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, APLICANDO LA METODOLOGÍA MAGERIT PARA EL GOBIERNO REGIONAL PUNO
CASO: PROYECTO ESPECIAL CAMÉLIDOS SUDAMERICANOS – PECSA, 2017

PROBLEMA GENERAL	OBJETIVO GENERAL	HIPOTESIS PRINCIPAL	VARIABLES	DISEÑO METODOLOGICO
¿Cómo establecer un Sistema de Gestión de Seguridad de la Información en el Proyecto Especial Camélidos Sudamericanos del Gobierno Regional Puno aplicando la Metodología MAGERIT, 2017?	Proponer un Sistema de Gestión de Seguridad de la Información, aplicando la metodología MAGERIT para el Gobierno Regional Puno, Caso: Proyecto Especial Camélidos Sudamericanos – PECSA, 2017.	La propuesta de un Sistema de Gestión de Seguridad de la Información es adecuada para el Proyecto Especial Camélidos Sudamericanos (PECSA) del Gobierno Regional Puno; Aplicando la Metodología Magerit, influirá de forma positiva	**Variables e Indicadores** Para demostrar y comprobar la hipótesis anteriormente formulada, la operacionalizamos, determinando las variables e indicadores que a continuación se mencionan. **Variable:** Sistema de Gestión de Seguridad de la Información	**Metodología** **Tipo de Investigación:** Documental y Descriptiva Según Bernal Torres (2010) La investigación documental consiste en un análisis de la información escrita sobre un determinado tema, con el propósito de establecer relaciones, diferencias, etapas, posturas o estado actual del conocimiento respecto al tema objeto de estudio. Según Niño Rojas (2011) La investigación descriptiva su propósito es describir la realidad objeto de estudio, un aspecto de ella, sus partes, sus clases, sus categorías o las relaciones que se pueden establecer entre varios objetos, con el fin de esclarecer una verdad, corroborar un enunciado o comprobar una hipótesis. Se entiende como el acto de representar por medio de palabras las características de fenómenos, hechos, situaciones, cosas, personas y demás seres vivos, de tal manera que quien lea o interprete, los evoque en la mente. **Método de la Investigación** Bernal Torres (2010) Los investigadores que utilizan el método cualitativo buscan entender una situación social como un todo, teniendo en cuenta sus propiedades y su dinámica. En su forma general, la investigación cuantitativa parte de cuerpos teóricos aceptados por la comunidad científica, en tanto que la investigación cualitativa pretende conceptuar sobre la realidad, con base en la información obtenida de la población o las personas estudiadas. **Diseño:** No experimental Según Hernández Sampieri (2014) La investigación no experimental es sistemática y empírica en la que las variables independientes no se manipulan porque ya han sucedido. Las inferencias sobre las relaciones entre variables se realizan sin intervención o influencia directa, y dichas relaciones se observan tal como se han dado en su contexto natural. **Área de estudio:** Proyecto Especial Camélidos Sudamericanos – PECSA del Gobierno Regional Puno **Población y Muestra** Personal Administrativo y Personal Técnico **Técnicas e Instrumentos.** La Entrevista.
PROBLEMAS ESPECIFICOS	**OBJETIVOS ESPECIFICOS**			
a. ¿Cómo es la situación actual del Proyecto Especial Camélidos Sudamericanos del Gobierno Regional Puno en relación a la Seguridad de la Información, 2017?	**a.** Conocer la situación actual del Proyecto Especial Camélidos Sudamericanos (PECSA) del Gobierno Regional Puno, respecto a la Seguridad de la Información, 2017.			
b. ¿Cómo son los activos de la Seguridad de la Información en los principales procesos identificados en el Proyecto Especial Camélidos Sudamericanos del Gobierno Regional Puno, aplicando la metodología Magerit, 2017?	**b.** Conocer los activos de la Seguridad de la Información, en el Proyecto Especial Camélidos Sudamericanos (PECSA) del Gobierno Regional Puno aplicando la metodología Magerit, 2017.			
c. ¿Cómo controla el Sistema de Gestión de la Seguridad de la Información en el Proyecto Especial Camélidos Sudamericanos del Gobierno Regional Puno, 2017?	**c.** Conocer los controles del Sistema de Gestión de la Seguridad de la Información en el Proyecto Especial Camélidos Sudamericanos (PECSA) del Gobierno Regional Puno, 2017.			
d. ¿Cómo es la mejor propuesta de una política y controles de seguridad en un Sistema de Gestión de Seguridad de la Información en el Proyecto Especial Camélidos Sudamericanos del Gobierno Regional Puno, basándonos con la metodología Magerit, 2017?	**d.** Conocer una Política y Manual del Sistema de Gestión de la Seguridad de la Información en el Proyecto Especial Camélidos Sudamericanos (PECSA) del Gobierno Regional Puno, basándonos con la metodología Magerit, 2017.			

ANEXO 2: Matriz de Operacionalización

VARIABLE	DIMENSIONES	INDICADORES	ITEMS		INSTRUMENTO	ESCALA DE MEDICIÓN
Sistema de Gestión de Seguridad de la Información	Organización de la seguridad de la información	Roles y responsabilidades para la seguridad de la información	1	¿Existe algún tipo de rol o responsabilidad para el resguardo de la seguridad de la información? Mencione	Entrevista	Descriptivo
			2	¿Existe un compromiso por parte del representante de la alta dirección con respecto a la Seguridad de la Información? Describa.		
	Seguridad de los recursos humanos	Toma de conciencia, educación y formación en la seguridad de la información	3	¿Se tiene un proceso disciplinario formal y comunicado para tomar acciones contra empleados que hayan cometido una infracción a la seguridad de la información? Describa cómo.		
		Términos y condiciones del empleo	4	¿Los empleados al finalizar su contrato como dejan clasificada su información?		
	Gestión de activos	Inventario de activos	5	¿Cómo se tiene identificado todos los activos de la institución?		
		Directrices de clasificación	6	¿Cómo se tiene clasificado la información de toda la institución?		
	Control de acceso	Políticas de control de acceso	7	En la institución del PECSA. ¿Se tiene limitado el acceso a la información? Indique		
		Gestión de derechos de acceso privilegiados	8	¿Los usuarios cambian sus contraseñas con frecuencia para acceder a un sistema o computadora?		
	Seguridad física y ambiental	Control de ingreso físico	9	¿Cuáles son las protecciones contra las amenazas externas y ambientales (Desastres naturales)?		
		Mantenimiento de equipos	10	¿Realizan un mantenimiento preventivo a los equipos informáticos de la institución? Cada cuanto tiempo.		
	Seguridad de las operaciones	Respaldo de la información	11	¿Se realiza copias de respaldo de la información del personal que labora en el proyecto?		
		Restricciones sobre la instalación de software	12	¿Cuáles son los controles o restricciones para los usuarios que quieran instalar algún tipo de software?		
	Seguridad de las comunicaciones	Controles de red	13	¿La red de datos de la institución es controlada para proteger la información? Cómo.		
		Seguridad de Servicios de Red	14	¿Existe algún mecanismo de seguridad para todos los servicios con acceso a la red? Menciones.		
	Cumplimiento	Protección de registros	15	¿Los datos e información del personal están protegidos de cualquier perdida, destrucción, falsificación y acceso no autorizado?		
		Cumplimiento de políticas y normas de seguridad	16	¿El director revisa regularmente el cumplimiento de la política, procedimientos y normas de la información?		

ANEXO 3: Formato de Entrevista

El presente instrumento tiene el propósito de obtener información relacionada con su opinión sobre el tema en estudio de esta investigación que es:
Propuesta de un Sistema de Gestión de Seguridad de la Información, Aplicando la Metodología MAGERIT para el Gobierno Regional Puno
Caso: Proyecto Especial Camélidos Sudamericanos – PECSA, 2017

Información General:

Nombre del Entrevistado: ……..……..…
Edad: ……. Puesto laboral: ……
Tiempo que labora en el Proyecto Especial Camélidos Sudamericanos: ……

1. **Organización de la seguridad de la información**

   ¿Existe algún tipo de rol o responsabilidad para el resguardo de la seguridad de la información? Mencione

   _____
   _____

   ¿Existe un compromiso por parte del representante de la alta dirección con respecto a la Seguridad de la Información? Describa.

   _____
   _____

2. **Seguridad de los recursos humanos**

   ¿Se tiene un proceso disciplinario formal y comunicado para tomar acciones contra empleados que hayan cometido una infracción a la seguridad de la información? Describa cómo.

   _____
   _____

   ¿Los empleados al finalizar su contrato como dejan clasificada su información?

   _____
   _____

3. **Gestión de activos**

   ¿Cómo se tiene identificado todos los activos de la institución?

   _____
   _____

   ¿Cómo se tiene clasificado la información de toda la institución?

   _____
   _____

4. **Control de acceso**

   En la institución del PECSA. ¿Se tiene limitado el acceso a la información? Indique.

   _____
   _____

¿Los usuarios cambian sus contraseñas con frecuencia para acceder a un sistema o computadora?

_____
_____

5. Seguridad física y ambiental

¿Cuáles son las protecciones contra las amenazas externas y ambientales (Desastres naturales)?

_____
_____

¿Realizan un mantenimiento preventivo a los equipos informáticos de la institución? Cada cuanto tiempo.

_____
_____

6. Seguridad de las operaciones

¿Se realiza copias de respaldo de la información del personal que labora en el proyecto?

_____
_____

¿Cuáles son los controles o restricciones para los usuarios que quieran instalar algún tipo de software?

_____
_____

7. Seguridad de las comunicaciones

¿La red de datos de la institución es controlada para proteger la información? Cómo.

_____
_____

¿Existe algún mecanismo de seguridad para todos los servicios con acceso a la red? Menciones.

_____
_____

8. Cumplimiento

¿Los datos e información del personal están protegidos de cualquier perdida, destrucción, falsificación y acceso no autorizado?

_____
_____

¿El director revisa regularmente el cumplimiento de la política, procedimientos y normas de la información?

_____
_____

ANEXO 4: Validación de Instrumento

ANEXO N° 04

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LOS INSTRUMENTOS

N°	Dimensiones / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. Organización de la seguridad de la información	Si	No	Si	No	Si	No	
1	¿Existe algún tipo de rol o responsabilidad para el resguardo de la seguridad de la información? Mencione	✓		✓		✓		
2	¿Existe un compromiso por parte del representante de la alta dirección con respecto a la Seguridad de la Información? Describa.	✓		✓		✓		
	II. Seguridad de los recursos humanos	Si	No	Si	No	Si	No	Sugerencias
3	¿Se tiene un proceso disciplinario formal y comunicado para tomar acciones contra empleados que hayan cometido una infracción a la seguridad de la información? Describa cómo.	✓		✓		✓		
4	¿Los empleados al finalizar su contrato como dejan clasificada su información?	✓		✓		✓		
	III. Gestión de activos	Si	No	Si	No	Si	No	Sugerencias
5	¿Cómo se tiene identificado todos los activos de la institución?	✓		✓		✓		
6	¿Cómo se tiene clasificado la información de toda la institución?	✓		✓		✓		
	IV. Control de acceso	Si	No	Si	No	Si	No	Sugerencias
7	En la institución del PECSA. ¿Se tiene limitado el acceso a la información? Indique.	✓		✓		✓		
8	¿Los usuarios cambian sus contraseñas con frecuencia para acceder a un sistema o computadora?	✓		✓		✓		
	V. Seguridad física y ambiental	Si	No	Si	No	Si	No	Sugerencias
9	¿Cuáles son las protecciones contra las amenazas externas y ambientales (Desastres naturales)?	✓		✓		✓		
10	¿Realizan un mantenimiento preventivo a los equipos informáticos de la institución? Cada cuanto tiempo.	✓		✓		✓		
	VI. Seguridad de las operaciones	Si	No	Si	No	Si	No	Sugerencias
11	¿Se realiza copias de respaldo de la información del personal que labora en el proyecto?	✓		✓		✓		
12	¿Cuáles son los controles o restricciones para los usuarios que quieran instalar algún tipo de software?	✓		✓		✓		
	VII. Seguridad de las comunicaciones	Si	No	Si	No	Si	No	Sugerencias
13	¿La red de datos de la institución es controlada para proteger la información? Cómo.	✓		✓		✓		
14	¿Existe algún mecanismo de seguridad para todos los servicios con acceso a la red? Menciones.	✓		✓		✓		
	VIII. Cumplimiento	Si	No	Si	No	Si	No	Sugerencias
15	¿Los datos e información del personal están protegidos de cualquier perdida, destrucción, falsificación y acceso no autorizado?	✓		✓		✓		
16	¿El director revisa regularmente el cumplimiento de la política, procedimientos y normas de la información?	✓		✓		✓		

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [X] No aplicable [.....]

Apellidos y Nombres del Juez Validador. Dr/Mg: CHRISTIAN OVALLE PAULINO

DNI: 40234321 Especialidad del Validador: Ing. de Sistemas.

02 de Diciembre del 2017

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante
Especialidad

ANEXO 5: Política del Sistema de Gestión de Seguridad de la Información

POLÍTICA DEL SGSI

PECSA, entendiendo la importancia de una adecuada Gestión de la Información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para PECSA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados, asumiendo los siguientes compromisos:

- ✓ Minimizar el riesgo en las funciones más importantes de la entidad.
- ✓ Cumplir con los principios de seguridad de la información.
- ✓ Mantener la confianza de sus clientes, socios y empleados.
- ✓ Apoyar la innovación tecnológica.
- ✓ Proteger los activos tecnológicos.
- ✓ Establecer los procedimientos e instructivos en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios
- ✓ Terceros, clientes y todo colaborador interno – externo.
- ✓ Garantizar la continuidad del negocio frente a incidentes.
- ✓ Cumplir con la mejora continua y requerimientos regulatorios. legales y todo convenio que la entidad suscriba en función del Sistema de Gestión de Seguridad de la Información

_____

Director Ejecutivo del PECSA

30 de noviembre 2017 REVISIÓN: 00

Anexo 06: Manual del Sistema de Gestión de Seguridad de la Información

MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

ELABORADO POR:	WILLIAM YANA VIVEROS	
FECHA:	15-11-2017	
REVISADO POR:	FIDEL ELIGIO BARRIGA SERRUTO	
FECHA:	16-11-2017	
REVISADO POR:	LEONEL TITO ROSAS	
FECHA:	17-11-2017	
APROBADO POR:	ABEL ROGER CAMA TOVAR	
FECHA:	18-11-2017	

TABLA DE CONTENIDO

1. INTRODUCCION

La política de alto nivel o política general, aborda la necesidad de la implementación de un sistema de gestión de seguridad de la información (SGSI) planteado desde la descripción del quién, qué, por qué, cuándo y cómo, en torno al desarrollo de la implementación del SGSI.

Es así como, teniendo en cuenta la importancia que tiene que la entidad defina las necesidades de sus grupos de interés, y la valoración de los controles precisos para mantener la seguridad de la información, se debe establecer una política que tenga en cuenta el marco general del funcionamiento de la entidad, sus objetivos institucionales, sus procesos misionales, y que este adaptada a las condiciones específicas y particulares de cada una según corresponda para que sea aprobada y guiada por la Dirección.

De esta forma, una buena política es concisa, fácil de leer y comprender, flexible y fácil de hacer cumplir para todos aquellos dentro del alcance sin excepción. Son cortas, y enmarcan los principios que guían las actividades dentro de la entidad

2. OBJETIVO Y ALCANCE

El Manual del Sistema de Gestión de la Seguridad de la Información de PECSA está basado en la Metodología MAGERIT, en esta norma se encuentran plasmadas las especificaciones para la creación de un sistema de gestión de la seguridad de la información (SGSI). El manual tiene por objeto recoger, analizar y definir los diferentes lineamientos que rigen al Sistema de Gestión de Seguridad de la Información de PECSA.

3. CONTROL DEL MANUAL

Es responsabilidad el Ingeniero de Sistemas - Sistematizador lo concerniente a su elaboración, modificación, distribución y control. Además, este documento es propiedad exclusiva de la compañía y está prohibida su distribución o copia sin previa autorización de los responsables.

3.1 DISTRIBUCIÓNDEL MANUAL

Se editó una única versión del manual para la intranet de la empresa, para la fácil consulta de todos los funcionarios de esta.

3.2 REVISIÓN DEL MANUAL

Este documento será revisado como mínimo una vez al año para efectos de actualización, o por cualquier otro motivo que arroje resultados diferentes a los planeados por el Sistema de Gestión de Seguridad de la Información de la compañía.

4. POLITICA DE SGSI

PECSA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para PECSA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados, asumiendo los siguientes compromisos:

- ✓ Minimizar el riesgo en las funciones más importantes de la entidad.
- ✓ Cumplir con los principios de seguridad de la información.
- ✓ Mantener la confianza de sus clientes, socios y empleados.
- ✓ Apoyar la innovación tecnológica.
- ✓ Proteger los activos tecnológicos.
- ✓ Establecer los procedimientos e instructivos en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, Terceros, clientes y todo colaborador interno – externo.
- ✓ Garantizar la continuidad del negocio frente a incidentes.
- ✓ Cumplir con la mejora continua y requerimientos regulatorios. legales y todo convenio que la entidad suscriba en función del Sistema de Gestión de Seguridad de la Información.

5. PLANIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Las etapas definidas para el desarrollo y la implementación del Sistema de Gestión de Seguridad de la Información son:

a) Documentar el SGSI

b) Implementar el SGSI

c) Evaluar el SGSI a través de auditorías internas y externas

d) Mejorar continuamente la eficacia del SGSI a través de del análisis de datos.

6. ENFOQUE ORGANIZACIONAL PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS

6.1 METODOLOGIA PARA EL ANÁLISIS Y GESTIÒN DE RIESGOS

Para hacer la valoración de riesgos de seguridad de la información de PECSA se eligió metodología MAGERIT – versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Desarrollada por El Consejo Superior de Administración Electrónica del gobierno español. Se eligió esta metodología porque brinda una aproximación metódica con

herramientas que no dejan lugar a la improvisación. A lo largo del desarrollo de la metodología se establece además un paralelo con la metodología de medición de riesgo operativo de la compañía para así poder comparar los riesgos de seguridad de la información con los demás riesgos operativos de la compañía.

6.2 ANÁLISIS DE RIESGOS

Los criterios a realizar son:

a) Determinación de Activos: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

   Teniéndose activos como:

   - **Datos** que materializan la información
   - **Servicios** auxiliares que se necesitan para poder organizar el sistema.
   - **Las aplicaciones informáticas** *(software)* que permiten manejas los datos.
   - **Los equipos informáticos** *(hardware)* y que permitan hospedar datos, aplicaciones y servicios.
   - **Los soportes de información** que son dispositivos de almacenamiento d datos.
   - **El equipamiento auxiliar** que complementa el material informático.
   - **Las redes de comunicaciones** que permitan intercambiar datos.
   - **Las instalaciones** que acogen equipos informáticos y de comunicaciones.
   - **Las personas** que explotan u operan todos los elementos anteriormente citados.

   No todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y salvaguardas son diferentes.

b) Caracterización de las Dimensiones del Activo: De un activo puede interesar calibrar diferentes dimensiones:

   - Su **confidencialidad:** ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
   - Su **integridad:** ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcial-mente falsos o, incluso, faltar datos.
   - Su **disponibilidad:** ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.

- La **autenticidad:** ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

  Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar)

- La **trazabilidad** del uso del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?

  La **trazabilidad** del acceso a los datos: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

c) Valoración de los Activos: La valoración se puede ver desde la perspectiva de la '**necesidad de proteger**' pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes. El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un es-quema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

El valor nuclear suele estar en la información que el sistema maneja y los servicios que se prestan (activos denominados esenciales), quedando los demás activos subordinados a las necesidades de explotación y protección de lo esencial.

- ***Estimación del impacto*** Se puede calcular el impacto en base a tablas sencillas de doble entrada:

impacto		*degradación*		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Aquellos activos que reciban una calificación de impacto muy alto (MA) deberían ser objeto de atención inmediata.

- ***Estimación del riesgo:*** Por otra parte se modelan impacto, probabilidad y riesgo por medio de escalas cualitativas:

escalas		
impacto	probabilidad	riesgo
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Pudiendo combinarse impacto y frecuencia en una tabla para calcular el riesgo:

riesgo		***probabilidad***				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

d) Determinación de Amenazas: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

- **De origen natural**

Hay accidentes naturales (terremotos, inundaciones, ...). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.

- **Del entorno (de origen industrial)**

Hay desastres industriales (contaminación, fallos eléctricos, ...) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.

- **Defectos de las aplicaciones**

Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, 'vulnerabilidades'[13].

- **Causadas por las personas de forma accidental**

Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

- **Causadas por las personas de forma deliberada**

Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

No todas las amenazas afectan a todos los activos[14], sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

e) Salvaguardas: Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otra seguridad física y, por último, está la política de personal.

6.3 TRATAMIENTO DE LOS RIESGOS

El tratamiento de los riesgos permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume.

A. Opciones de tratamiento del riesgo: Eliminación

La eliminación de la fuente de riesgo es una opción frente a un riesgo que no es aceptable.

En un sistema podemos eliminar varias cosas, siempre que no afecten a la esencia de la Organización. Es extremadamente raro que podamos prescindir de la información o los servicios esenciales por cuanto constituyen la misión de la Organización. Cambiar estos activos supone reorientar la misión de la Organización.

Más viable es prescindir de otros componentes no esenciales, que están presentes simple y llanamente para implementar la misión, pero no son parte constituyente de la misma. Esta opción puede tomar diferentes formas:

- ✓ Eliminar cierto tipo de activos, emplean otros en su lugar. Por ejemplo: cambiar de sistema operativo, de fabricante de equipos.
- ✓ Reordenar la arquitectura del sistema (el esquema de dependencias en nuestra terminología) de forma que alteremos el valor acumulado en ciertos activos expuestos a grandes amenazas. Por ejemplo: segregar redes, desdoblar equipos para atender a necesidades concretas, alejando lo más valioso de lo más expuesto.

Las decisiones de eliminación de las fuentes de riesgo suponen realizar un nuevo análisis de riesgos sobre el sistema modificado.

B. Opciones de tratamiento del riesgo: Mitigación

La mitigación del riesgo se refiere a una de dos opciones:

- ✓ Reducir la degradación causada por una amenaza (a veces se usa la expresión 'acotar el impacto')
- ✓ Reducir la probabilidad de que una amenaza de materializa

En ambos casos lo que hay que hacer es ampliar o mejorar el conjunto de salvaguardas. En términos de madurez de las salvaguardas: subir de nivel.

Algunas salvaguardas, notablemente las de tipo técnico, se traducen en el despliegue de más equipamiento que se convierte a su vez en un activo del sistema. Estos nuevos activos también acumularán valor del sistema y estarán a su vez sujetos a amenazas que pueden perjudicar a los activos esenciales. Hay pues que repetir el análisis de riesgos, ampliándolo con el nuevo despliegue de medios y, por supuesto, cerciorarse de que el riesgo del sistema ampliado es menor que el del sistema original; es decir, que las salvaguardas efectivamente disminuyen el estado de riesgo de la Organización.

C. Opciones de tratamiento del riesgo: Compartición

Tradicionalmente se ha hablado de 'transferir el riesgo. Como la transferencia puede ser parcial o total, es más general hablar de 'compartir el riesgo.

Hay dos formas básicas de compartir riesgo:

- ✓ Riesgo cualitativo: se comparte por medio de la externalización de componentes del sistema, de forma que se reparten responsabilidades: unas técnicas para el que opera el componen-te técnico; y otras legales según el acuerdo que se establezca de prestación del servicio.
- ✓ Riesgo cuantitativo: se comparte por medio de la contratación de seguros, de forma que a cambio de una prima, el tomador reduce el impacto de las posibles amenazas y el asegurador corre con las consecuencias. Hay multitud de tipos y cláusulas de seguros para concretar el grado de responsabilidad de cada una de las partes.

Cuando se comparten riesgos cambia, bien el conjunto de componentes del sistema, bien su valoración, requiriéndose un nuevo análisis del sistema resultante.

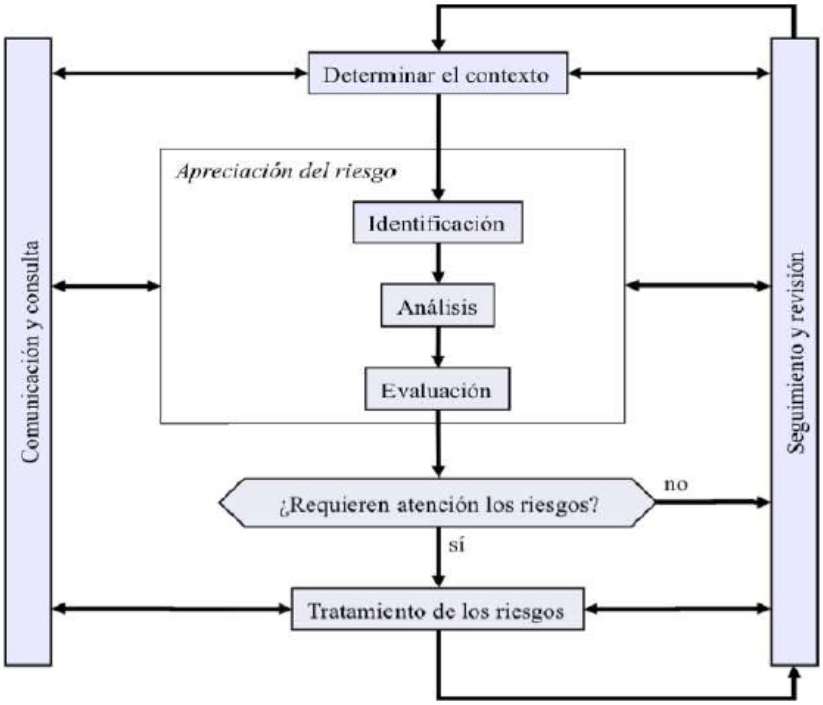
D. *Opciones de tratamiento del riesgo: Financiación*

Cuando se acepta un riesgo, la Organización hará bien en reservar fondos para el caso de que el riesgo se concrete y haya que responder de sus consecuencias. A veces de habla de fondos de contingencia y también puede ser parte de los contratos de aseguramiento.

Normalmente esta opción no modifica nada del sistema y nos vale el análisis de riesgos disponible.

6.4 PLAN DE TRATAMIENTO DE RIESGOS DEL SGSI

Después de efectuar los análisis de riesgos el comité de seguridad de la información junto con cada una de las áreas involucradas debe efectuar un plan de tratamiento de riesgos, para los riesgos considerados como críticos en los activos bajo su responsabilidad, los planes de tratamiento de riesgos deben ser registrados en el siguiente formato y serán administrados por el departamento de Sistemas:



7. REQUISITOS DE DOCUMENTACIÓN

Los parámetros de gestión documental de PECSA se encuentran definidos con las siguientes acciones de gestión necesarias para:

a) Aprobar los documentos en cuanto a su suficiencia antes de su publicación.
b) Revisar y actualizar los documentos según sea necesario y reprobarlos.
c) Asegurar que los cambios y el estado de actualización de los documentos estén identificados.
d) Asegurar que las versiones más recientes de los documentos pertinentes están disponibles en los puntos de uso.
e) Asegurar que los documentos permanezcan legibles y fácilmente identificables.
f) Asegurar que los documentos estén disponibles para quienes los necesiten, y que se apliquen los procedimientos pertinentes, de acuerdo con su clasificación, para su transferencia, almacenamiento y disposición final.
g) Asegurar que los documentos de origen externo estén identificados.
h) Asegurar que la distribución de documentos esté controlada.
i) Impedir el uso no previsto de los documentos obsoletos, y
j) Aplicar la identificación adecuada a los documentos obsoletos, si se retienen para cualquier propósito

8. IDENTIFICACIÓN DE DOCUMENTOS PARA EL SSGSI

PECSA establece y mantiene una metodología de implementación de controles, en función de las Salvaguardas Criticas, determinado así la siguiente documentación:

8.1 Procedimiento de Asignación de equipos y acceso de sistemas de Información.

8.2 Procedimiento de Desarrollo y actualización de sistemas de información

8.3 Procedimiento de respaldos de la información

8.4 Procedimiento de Seguridad de Redes.

8.5 Procedimiento de Gestión de Incidentes de Seguridad de la Información.

8.6 Procedimiento de Monitoreo de Red y Servicios

8.7 Procedimiento de Actualización de Sistemas Operativos y Software

8.8 Procedimiento de Auditorías Internas de Seguridad de la Información.

8.9 Procedimiento de Acciones Correctivas y Preventivas

9. SEGUIMIENTO Y REVISIÓN DEL SGSI

PECSA establece como control interno la aplicación del seguimiento y revisión del SGSI, de forma Mensual, para el cumplimiento estricto del cumplimiento del Sistema de Gestión de la Seguridad de la Información.

9.1 AUDITORÍAS INTERNAS DEL SGSI

PECSA establece una metodología de Auditorías Internas de Seguridad de la información. Allí se define la responsabilidad y autoridad en las auditorías de Seguridad de la Información. Esta metodología se encuentra registrada en el documento: "Auditorías Internas de seguridad de la información"

9.2 INDICADORES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Se definen los siguientes indicadores para medir los objetivos del sistema de gestión de seguridad de la información de PECSA:

- ✓ Gestión de Riesgos de Seguridad
- ✓ Gestión Segura del Riesgo Humano
- ✓ Seguridad de Aplicaciones Acceso
- ✓ Continuidad
- ✓ Seguridad en Operaciones

9.3 REVISIÓN DEL SGSI POR LA DIRECCIÓN

La Alta Gerencia PECSA, revisará, a través del Comité de Seguridad de la Información, la efectividad de la implementación del Sistema de Gestión de Seguridad de la Información y el comportamiento de sus indicadores cada vez que se estime conveniente y de acuerdo con los resultados mostrados, se hará una vez cada año. Los temas que serán tratados de forma obligatoria son:

Aspectos	Registro
Revisión de la política y objetivos del sistema de gestión	Acta
Resultados del análisis de riesgos y seguimiento a los planes de tratamiento establecidos	Seguimiento plan de tratamiento de riesgos
Evaluación de conformidad con los requisitos legales aplicables	Acta
Estado de investigación y análisis de incidentes de seguridad de la información	Acta
Resultados de auditorías internas	Informe de auditorías internas
Acciones correctivas y preventivas	Acta
Cambios al Sistema de Gestión de seguridad de la información	Acta
Recomendaciones para la mejora	Acta
Seguimiento de revisiones previas	Acta
Desempeño financiero y costos relacionados con la seguridad de la información	Acta
Necesidad de recursos	Acta

10. MEJORA DEL SGSI

Todas las áreas, según la información recolectada, se encargan de trazar planes para el mejoramiento continuo de acuerdo con la Política y Objetivos de Seguridad de la Información. El director Ejecutivo y el Comité de Seguridad de la Información participan activamente en el desarrollo y evaluación de estos planes.

Se deben revisar y monitorear los siguientes elementos que componen en el SGSI:

- ✓ Contenido de los procedimientos:

Creación, modificación y actualización de los procedimientos tanto en estructura como en contenido, buscando la descripción real de cada una de las actividades que se desarrollan dentro de la organización. Lo anterior incluye: descripciones, caracterización, controles, objetivos, formatos, entre otros.

- ✓ Contenido Intranet:

Actualización y modificación del contenido de la Intranet según las modificaciones de los procesos y la creación de los mismos.

- ✓ Manual SGSI:

|Actualización o modificación del manual por las siguientes razones:

- ✓ Cambios en normatividad de entes externos.
- ✓ Cambios en la metodología (riesgos, controles fuentes de información, etc.).
- ✓ Cambios o inclusión de estrategias.
- ✓ Cambios por determinación de entes de control interno.
- ✓ Cambios por estructura organizacional.

Evolución del riesgo en el tiempo, es decir, si con la aplicación de controles ha ido disminuyendo. Conjunto de descripciones detalladas de los incidentes, por proceso, funcionario y área.

10.1 ACCIONES CORRECTIVAS Y PREVENTIVAS

Este procedimiento aplica a todo el Sistema de Gestión de seguridad de la Información de PECSA y se inicia con la identificación de la no-conformidad hasta que es eliminada o la no conformidad potencial existente hasta que es controlada.

a) Acción correctiva: acción implementada para lograr la eliminación de una no-conformidad detectada.
b) Acción preventiva: acción tomada para eliminar la causa de una no-conformidad potencial u otra situación potencial indeseable.
c) Corrección: acción tomada para eliminar la no-conformidad.
d) No conformidad: incumplimiento de un requisito del SGSI.

PECSA buscará el mejoramiento continuo del Sistema de Gestión de seguridad de la información, detectando las no-conformidades reales o potenciales que pudieran afectar su operación.

Los problemas existentes (no-conformidades reales) pueden ser detectados por cualquiera de las siguientes formas:

- ✓ Registro de incidentes
- ✓ Observaciones en las auditorias de seguridad de la información
- ✓ Bajos índices de gestión en cualquiera de las áreas de la compaña
- ✓ Observaciones hechas por los mismos colaboradores de la compaña

Los problemas que pueden convertirse en no-conformidades (no-conformidades potenciales) pueden ser encontrados en cualquiera de las siguientes actividades:

- ✓ Comentarios de los clientes
- ✓ Observaciones de los clientes en las encuestas de satisfacción
- ✓ Observaciones realizadas a través de las auditorias de seguridad de la información
- ✓ Tendencias en los índices de gestión de las áreas
- ✓ Observaciones hechas por los mismos colaboradores de la compaña

11. PROGRAMAS DE FORMACIÓN Y TOMA DE CONCIENCIA

Brindar a los funcionarios de PECSA, y a los terceros, el Manual del SGSI, los procedimientos, la política y demás elementos teóricos y prácticos que faciliten la correcta implementación del Sistema de Gestión de Seguridad de la Información en la Compañía.

- ✓ Realizar capacitaciones a todos los funcionarios de la empresa de forma anual evaluando el alcance de los objetivos propuestos y su eficacia.
- ✓ Realizar capacitaciones a los nuevos funcionarios durante el periodo de inducción.
- ✓ Publicar todos los documentos, normas, procesos y demás temas relacionados, en lugares donde todos los funcionarios los puedan consultar y se puedan mantener actualizados (Intranet y/o carteleras).
- ✓ Mantener toda la documentación actualizada mediante la continua revisión, por parte de las personas que se encuentran involucradas en los procesos.

12. CONTROL DEL DOCUMENTO

CONTROL DEL DOCUMENTO	
Nº de Versión	**Descripción del Cambio**
----	--------