UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

FACULTAD DE INGENIERÍA INDUSTRIAL, SISTEMAS E INFORMÁTICA

ESCUELA PROFESIONAL DE INGENIERÍA INFORMATICA

TESIS

SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA MUNICIPALIDAD PROVINCIAL DE HUARAL

Para optar el título profesional de Ingeniero Informático

Presentado por los Bachilleres:

TENORIO ARQUE, ABRAHAM MARCOS

RIVAS MINAYA, JOSE ALBERTO

Asesorado por:

Ing. Víctor Fredy, ESPEZUA SERRANO

Huacho, Perú

2017

DEDICATORIA

A Dios, por darnos la fuerza necesaria y permitirnos llegar a este nivel intelectual.

A nuestros padres por ser guías y apoyo, en todos los actos de bien y progreso que experimentamos en los caminos que vamos realizando.

A todos nuestros maestros por brindarnos su sabiduría y que con sus ejemplos de superación inspiran a sus discípulos.

Los Autores

Agradecimiento

A Dios gracias, el cual hace que siempre
Triunfe y logremos todo lo que
nos proponemos.
A nuestros padres que siempre nos brindan
lo mejor y siempre está apoyándonos
en todo momento para cumplir
cada meta trazada.

Los Autores.

INDICE GENERAL

CAPITULO III: METODOLOGIA

CAPITULO IV: SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA MUNICIPALIDAD PROVINCIAL DE HUARAL

CAPITULO V: VALIDACION DE INSTRUMENTOS Y RESULTADOS ESTADISTICOS

CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES

CAPITULO VII: FUENTES DE INFORMACION

ANEXOS

INDICE DE FIGURAS

INDICE DE TABLAS

SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA MUNICIPALIDAD PROVINCIAL DE HUARAL

INFORMATION SECURITY MANAGEMENT SYSTEM FOR THE PROVINCIAL MUNICIPALITY OF HUARAL

TENORIO ARQUE, Abraham Marcos[1], RIVAS MINAYA, José Alberto[1]

RESUMEN

Objetivo: Establecer la relación entre sistema de gestión de seguridad de información y las diversas amenazas físicas y lógicas existentes en la Municipalidad Provincial de Huaral. **Métodos:** Basado en un diseño no experimental, estudio intrínseco y holístico de un caso, que consiste en observar, tal como se da en su contexto natural y actual, el funcionamiento ya existente del sistema de gestión de seguridad de información para la municipalidad provincial de Huaral y en comprender todo el caso como una única unidad de análisis. **Resultados:** Los resultados muestran que más del 60% de encuestados están de acuerdo con la aplicación del sistema de gestión de seguridad de información y las diversas amenazas físicas y lógicas existentes en la Municipalidad Provincial de Huaral. **Conclusión**: Existe una confiabilidad positiva significativa de 0,862.

Palabras clave: sistema de gestión de seguridad de la información, amenazas físicas y lógicas.

ABSTRAC

Objective: To establish the relationship between the information security management system and the various physical and logical threats that exist in the Provincial Municipality of Huaral. **Methods:** Based on a non-experimental design, intrinsic and holistic study of a case, which consists of observing, as it occurs in its natural and current context, the existing functioning of the information security management system for the provincial municipality of Huaral and in understanding the whole case as a single unit of analysis. **Results:** The results show that more than 60% of respondents agree with the application of the information security management system and the various physical and logical threats that exist in the Provincial Municipality of Huaral. **Conclusion:** There is a significant positive reliability of 0.862.

Keywords: information security management system, physical and logical threats.

---

[1]Escuela Profesional de Ingeniería Informática. Facultad de Ingeniería Industrial, Sistemas e Informática. Universidad Nacional José Faustino Sánchez Carrión. Huacho-Perú.

INTRODUCCIÓN

En la presente tesis, se diseña la propuesta de un sistema de gestión de seguridad de información para la municipalidad provincial de Huaral y se encuentra ubicado dentro del área temática de industrias de la información y del conocimiento.

La seguridad de información, en términos generales es entendida como todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información, buscando de esta manera mantener la confidencialidad, la disponibilidad e integridad de la misma. Un activo de información es un activo que tiene un determinado valor para la organización, sus operaciones comerciales y su continuidad.

La característica principal de un sistema de gestión de seguridad de información es resguardar la integridad, confidencialidad e integridad de los activos de información en una organización; lo cual se logra a través de un minucioso análisis de los riesgos a los que están expuestos los activos de información para luego implantar los controles necesarios que ayudarán a proteger estos activos.

La problemática principal actual de las empresas que desean incursionar en el ámbito de servicios municipales es la falta de seguridad y la poca previsión respecto a los riesgos con la que cuentan sus activos de información. El resultado de no tener las medidas necesarias para mitigar estos riesgos puede llevar a la empresa a pérdidas no solo de información, sino también económica.

Es por ello, que la municipalidad provincial de Huaral, se ve en la necesidad de implementar un conjunto de herramientas, procedimientos, controles y políticas que aseguren la confidencialidad, disponibilidad e integridad de la información; con ellos

garantizar a que se acceda a la información solo por quienes estén designados para su uso, que esté disponible cuando requieran los que estén autorizados y permanezca tal y como fue creada por sus propietarios, y asegurar así también la actualización de la misma.

El presente trabajo consta de siete capítulos. Ellos son:

En el capítulo I se presenta el planteamiento del problema y los objetivos del proyecto

El capítulo II muestra el marco teórico, en el que están planteadas las bases teóricas relacionadas con un sistema de gestión de seguridad de la información (SGSI), definiciones de términos básicos que sustentan el desarrollo adecuado del trabajo y antecedentes de la investigación.

En el capítulo III se especifican los materiales, métodos y herramientas utilizadas para el desarrollo del trabajo de investigación. También se define la metodología a emplear, la cual es la resultante de un estudio de distintas metodologías y de la investigación y aporte de los autores de este trabajo de investigación.

El capítulo IV se presenta el sistema de gestión de seguridad de información que se propondría para la municipalidad provincial de Huaral,

El capítulo V se aborda la Validación de los instrumentos y el análisis y resultados estadísticos y discusión de los resultados a manera de explicación de los mismos, teniendo en cuenta las variables expuestas en los capítulos anteriores.

A partir de los resultados obtenidos se han planteado las conclusiones y recomendaciones pertinentes, y finalmente se consigna la bibliografía utilizada y los anexos respectivos.

CAPITULO I: PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la realidad problemática

Toda organización de hoy día busca principalmente llevar sus actividades de manera eficaz y con el menor uso de recursos económicos y humanos así también busca brindarle la mejor atención al cliente. Todo lo mencionado es debido a los grandes avances de la tecnología que ha desarrollado importantes herramientas que permiten realizar de manera más rápida actividades y operaciones específicas o rutinarias. Entre las ventajas que ha proporcionado la tecnología en el ámbito organizacional, se encuentran principalmente la automatización de procesos, administración organizada de la información de un área o departamento, aumentos considerables en la producción, entre otras.

Por lo tanto, estos factores se pueden prevenir gracias a un adecuado diseño de sistema de información que posteriormente se podrá implementar para mejorar la satisfacción al cliente.

Las organizaciones públicas día a día generan conocimientos, datos, reportes, actas y material de diferente índole de suma importancia para ellas, lo cual representa toda la información que requieren para su funcionalidad. Esta información en la mayoría de los casos, es almacenada en diferentes medios tanto físicos como electrónicos, además es puesta a disposición del personal que requiere hacer uso de esta información para toma de decisiones, realización de planes, reportes, inventarios, entre otros.

El acceso no autorizado a la información se ha vuelto más fácil debido a los tantos métodos existentes y nuevos para extraer información, esto ha permitido que sea más difícil salvaguardar la información y sus métodos de transmisión; ya sean estos comunicados verbales, archivos, documentos, base de datos, entre otros.

Por lo anteriormente citado es necesaria la implementación de herramientas, procedimientos, controles y políticas que aseguren la confidencialidad, disponibilidad e integridad de la información; con ellos garantizar a que accedan a la información quienes estén

designados para su uso, esté disponible cuando se requiera y permanezca tal como fue creada por sus propietarios y asegurar también la actualización de la misma.

Debido al crecimiento de los servicios que Implementa la Municipalidad Provincial de Huaral, la probabilidad de que la información sea interceptada, robada y/o modificada por personas inescrupulosas y sin autorización de acceso a esta, ha aumentado exponencialmente. Lo cual resulta peligroso para la organización, ya que mucha de la información fundamental e importante para la realización de los procesos críticos de los servicios puede ser vulnerada y amenazada ocasionando la interrupción de estos procesos; que conllevan, de esta manera, a una pérdida no solo de información, sino también financiera.

Por lo anteriormente citado es necesaria la implementación de herramientas, procedimientos, controles y políticas que aseguren la confidencialidad, disponibilidad e integridad de la información; con ellos garantizar a que accedan a la información quienes estén designados para su uso, esté disponible cuando se requiera y permanezca tal como fue creada por sus propietarios y asegurar también la actualización de la misma.

La Municipalidad Provincial de Huaral, a través de la Subgerencia de Tecnologías de la Información y Sistemas es la unidad orgánica de apoyo encargado de planificar, ejecutar y dirigir la implementación de las actividades relacionadas a la gestión de los recursos y las tecnologías de la información y comunicación de la Municipalidad. Así mismo, es la encargada de la Reparación y/o mantenimiento de equipos de cómputo sin garantía.

1.2 Formulación del problema

1.2.1 Problema general

¿Qué relación existe entre el sistema de gestión de seguridad de información y las diversas amenazas físicas y lógicas existentes en la Municipalidad Provincial de Huaral?

1.2.2 Problemas Específicos

¿En qué medida los desastres naturales, estructurales, Hardware, Software y otros procedimientos de seguridad de información Influirían en un Deficiente sistema de gestión de seguridad de información para la Municipalidad Provincial de Huaral?

¿En qué medida los altos niveles de riesgos, frente a las diversas amenazas físicas y lógicas Influirían en un Deficiente sistema de gestión de seguridad de información para la Municipalidad Provincial de Huaral?

1.3 Objetivos de la Investigación

1.3.1 Objetivo general

Establecer la relación entre sistema de gestión de seguridad de información y las diversas amenazas físicas y lógicas existentes en la Municipalidad Provincial de Huaral.

1.3.2 Objetivos específicos

- Implementar una Política de Seguridad de Información a fin de Reducir las diversas Amenazas físicas y lógicas existentes en la Municipalidad Provincial de Huaral.

- Determinar cómo Monitorear de manera Eficiente los Incidentes y Vulnerabilidades de Seguridad de la Información para Reducirlos en la Municipalidad Provincial de Huaral.

1.4 Viabilidad

1.4.1 Viabilidad técnica

Es técnicamente posible la implementación del sistema de gestión de seguridad de información por los siguientes motivos:

* El hardware a utilizar es compatible con la infraestructura actual de la organización, por lo que no se tendría problema para la implementación del proyecto.

* El software a utilizar, en su mayoría, serán propios de la organización; solo se adquirirán nuevas licencias y actualizaciones, por lo que no se tendría problemas para la implementación del proyecto.

* Todo el personal está capacitado con la infraestructura actual de la organización. las nuevas tecnologías que se adquirirán serán previamente capacitadas por el proveedor, por lo que no se tendría problemas para la implementación del proyecto.

1.4.2 Viabilidad económica

Es económicamente posible, ya que habría un el ahorro para la implementación del SGSI, así como su costo del proyecto.

1.4.3 Viabilidad social

* Beneficios a la sociedad

***** Impacto en el medio ambiente

Para la implementación de un SGSI, es necesario consumir diversos recursos adicionales que impactan en el medio ambiente, siendo estos:

* Generación de papeles

* Generación de residuos peligrosos: (tóner de impresoras, cintas de impresión de máquinas de escribir, etc.)

* Consumo de energía (luces generales e informática)

CAPITULO II: MARCO TEORICO

2.1 Antecedentes de la investigación

2.1.1 Antecedentes de la Municipalidad Provincial de Huaral

A. Reseña histórica

Huaral es fundado por los españoles en el año 1551, durante el virreinato de don Antonio de Mendoza Marqués de Mondejar, como Asiento de Naturales bajo la advocación de San Juan Bautista de Huaral en reemplazo de la población prehispánica llamada "Guaral Viejo" conformando por los ayllus dispersos llamados: Guaril, Huando, Jecuan, Huaca - Puquio, Huayan, Cuyo y otros. Esta fundación se hizo en cumplimiento de la Real Ordenanza española de 21 de marzo de 1551, que disponía que los aborígenes fuesen reducidos a pueblos y ciudades. Por ello, los ayllus dispersos de la margen derecha del río Chancay, fueron reunidos en “Huaral Nuevo”, Se crea como distrito, el 25 de octubre de 1890, después de haber permanecido 128 años en el ámbito territorial de Villa Chancay y el 31 de octubre lo promulgó el Presidente de la República de entonces, Coronel Remigio Morales Bermúdez. Luego de 18 años de gestiones, se crea la provincia de Huaral el 11 de Mayo de 1976 con la aprobación de la Ley de Creación Nº 21488 suscrita por el entonces Presidente de la República, el General EP Francisco Morales Bermúdez Cerrutti, por coincidencia, nieto del Presidente que creó el distrito de Huaral, siendo alcalde del distrito de Huaral el Ing. José Pinasco Elguera, que pasa a ser el primer Alcalde provincial y a fines del mes de junio de ese mismo año asume ese cargo el Sr. Carlos Mora Parra, quien fue uno de los principales gestores para la creación de la Provincia de Huaral. Cabe destacar al Dr. Teodoro Cassana Robles, abogado canteño, su importante intervención para este propósito, porque convenció a sus paisanos de la necesidad de la nueva provincia. La realidad era que la mayoría de las localidades serranas designadas para pasar a Huaral, estaban más ligadas a Huaral,

la futura provincia, que a Canta o a Huacho. Se designó como su capital a la ciudad de Huaral.

B. Visión y Misión

B.1 Visión

Nuestra Visión es que en el 2021 Huaral se consolide como provincia turística, ecológica y agroexportadora en un marco de respeto al ciudadano. La Municipalidad Provincial de Huaral es un Gobierno Local Democrático, Representativo, Planificador y Concertador que liderará y contribuirá a elevar la calidad de vida de su población.

B.2 Misión

Somos una institución municipal promotora del desarrollo, con recursos humanos calificados. Buscamos alcanzar estándares óptimos de gestión en desarrollo urbano, rural, económico y social, con mecanismos que promueven la participación de la población y en alianza con el sector público y privado. En el marco de los lineamientos del Plan de Desarrollo Concertado de Huaral que permita mejorar la calidad de vida y alcanzar el desarrollo humano de los pobladores de Huaral.

C. Servicios que brinda

* Programas sociales
* Licencia de funcionamiento
* Licencia de edificación
* Tributos municipales
* Seguridad Ciudadana
* Defensa civil

* Adjudicación directa de rutas
* Licencias y papeletas
* Plan de desarrollo Urbano
* Registro civil
* Rentas en línea

2.1.2 Investigaciones Internacionales

a) Pítsica Marques, M. (2001). Tesis: S*istema de Información para la gestión aplicado en las entidades financieras.* Memoria para optar al grado de Doctor, Universidad Complutense de Madrid.

Conclusiones:

1. Un sistema de información surge para satisfacer las necesidades de información y comunicación de un grupo de personas. Su misión es promover que el saber que reside en cualquier lugar de una organización, se distribuya de forma conveniente a otros individuos y pase a ser un activo de la empresa. - El sistema debe, además, poseer la capacidad de "crecer", no es necesario que sea "grande" desde el principio; lo esencial es que "crezca" con el tiempo adaptándose al medio y a las necesidades de la organización.

2. Para que un sistema de información sea considerado soporte de la toma de decisiones, debe reunir una serie de características entre las que destacan: interactividad, tipo de decisiones, frecuencia de uso, variedad de usuarios, flexibilidad, incorporación de nuevos modelos, interacción ambiental, comunicación organizacional, acceso a las bases de datos y simplicidad. Estas cualidades facilitan de alguna manera el proceso de toma de decisiones.

3. El método de aplicación de desarrollo del sistema de información debe ser elegido mediante la observación de algunos aspectos dentro de la misma empresa, como coste / beneficio, desempeño interno, calidad, facilidad de adaptación, comodidad, rapidez, etc. En suma, debe propiciar al directivo ventajas suficientes para cubrir sus costes y justificar su implantación en la empresa.

4. Se puede estimar que el uso de los sistemas de información crecerá considerablemente dentro de las entidades financieras, siempre cambiando para cumplir de la mejor manera los objetivos de la entidad. Cabe recordar que los cambios tecnológicos dentro del sistema de información para la gestión han hecho que su propia denominación cambie (*CRM, Data warehouse,* etc)

5. Lo más importante es que la tecnología no pare de evolucionar y que un día pueda cumplir su papel pleno dentro de la organización: que el directivo se sienta satisfecho con su ayuda.

b. Viteri Jiménez, Mayra Johanna (2014) "*Políticas de seguridad informática en el Departamento de Tecnologías de la Información y comunicación en beneficio de la Universidad Técnica Estatal de Quevedo Manual de Procedimientos".* Tesis previa para obtención del título de ingeniería de sistemas, Universidad Técnica Estatal de Quevedo Ecuador. Lo cual tiene como objetivo definir políticas de seguridad informáticas en la UTEQ que conlleven a un mejor uso de los activos tecnológicos y la información. Esta propuesta está basada en la definición de políticas y estándares de la seguridad basada en la ISO 27001, misma que proporciona los controles necesarios para la implementación de un sistema de seguridad. La metodología de investigación que se llevó a cabo para este proyecto es el

método descriptivo, teniendo como finalidad la adquisición de datos objetivos, precisos y sistemáticos que pueden usarse en promedio. Y con lo preliminar mencionando se llegó a las siguientes conclusiones Se efectuó un análisis de riesgos informáticos mediante encuesta a todo personal de la Unidad de Tic para valorar los activos y así adecuar las políticas a la realidad de la institución. Se pudo concluir que las conexiones a Internet deben contar con elementos de prevención, detección de intrusos, filtros contra virus, manejo de contenidos, los mismos que afectan la integridad de los sistemas y la información institucional.

c. Jorge. G., & Cristian A. (2013) "Protocolo de Políticas de seguridad para las Universidades de Risaralda", Tesis previa a la Obtención del Título de: Ingeniero de Sistemas y Telecomunicaciones. Universidad Católica de Pereira Colombia, lo cual tiene por objetivo general un protocolo para la elaboración de una política de seguridad informática de la educación superior en Risaralda ya que la información juega un papel muy importante y es considerado el activo más valioso en todas las organizaciones, lo cual ha generado que se le dé mayor atención a la disponibilidad, confidencialidad e integridad segura y sistemas protegidos.

Por lo tanto, se hace necesario contar con estrategias y procedimientos a la hora de implementar la seguridad informática, para así garantizar el correcto funcionamiento de los sistemas y al momento de un posible ataque o desastre natural que conlleve a la perdida de información o sistemas informáticos, saber cómo actuar para mitigar el problema tomando los correcticos apropiados. Haciendo relación a las universidades de Risaralda, estas instituciones educativas de educación superior requieren de gran control en este aspecto, así como unas políticas bien establecidas en todo lo cierne a este aspecto, así como unas políticas bien establecida en todo lo que concierne al manejo de la información de datos y usuarios, que sean precavidas a la hora de permitir el acceso a los sistemas informáticos.

Las conclusiones más resaltantes de esta investigación es que la educación superior no se está rigiendo por ninguna norma de estandarización modelo como la norma ISO 27000 y la norma ISO 17000 que brindan una guía para el establecimiento e implementación adecuada de la seguridad informática, una de las principales debilidades reflejadas en la indagación realizada en campo mediante normativos y prácticos que permitan la evaluación de desempeño de los sistemas tecnológicos e informáticos, como lo son las auditorias y estudios de la red para establecer los riesgos, amenazas y vulnerabilidades presentes en estos.

d. Contreras S (2012), realizo la investigación: *desarrollo de un sistema de información para la adecuación de los procesos del departamento de almacén y logística en la empresa venezolana de construcción y mantenimiento vechaa c.a., Maturín estado monagas,* en la escuela de ingeniería de sistemas de la universidad de oriente núcleo de Monagas.

La investigación llego a las siguientes conclusiones:

* Por medio de la comunicación directa que se tuvo con la empresa, se facilitó el estudio de la situación actual presentada en el Departamento de Almacén y Logística, definiendo así los focos problemáticos y los requerimientos del sistema, mediante las necesidades planteadas por dicho departamento, se identificó como principal problema el descontrol en las entradas y salidas de los materiales que utilizan para los diferentes proyectos de trabajo.

* Luego del estudio directo en el departamento, se recolectó la información necesaria para describir los procesos llevados a cabo, señalando de esta manera las fallas existentes, como el desorden en la elaboración de reportes de inventario.

* A través de las necesidades y fallas presentadas por el departamento se pudo establecer las fases de desarrollo, siguiendo los lineamientos de la estructura operativa mixta planteada, creando un rediseño de los procesos a fin de adaptarlos a las necesidades del cliente y el desarrollador, llevando así procesos manuales a procesos automatizados.

* El adecuado diseño de la base de datos resultó fundamental en el desarrollo de la aplicación, y por medio de las diversas vistas de los diagramas elaborados se permitió definir y explicar las funciones del sistema, lo cual facilitó la adecuación de los procesos propuestos.

2.1.3 Investigaciones nacionales

1. Norabuena, A. (2011), realizo la investigación: *Análisis, diseño e implementación de un sistema de información para la gestión académica de un instituto superior tecnológico,* en la facultad de ciencias e ingeniería de la Universidad Católica del Perú.

La investigación llego a las siguientes conclusiones:

A. La metodología RUP en las fases elegidas para el desarrollo de este proyecto, tal como se indican en la sección 2.1.2, guiaron de forma efectiva el desarrollo del software en todas sus etapas, desde el análisis hasta la implementación, brindando un mecanismo fiable y eficiente que describía cada componente considerado para la implementación final.

B. Los conocimientos adquiridos durante los ciclos de estudio en la Facultad de Ciencias e Ingeniería de la Universidad se integraron y coadyuvaron a la conclusión satisfactoria de este trabajo. Pero, se debe considerar que gran parte de este conocimiento es de orientación general, y por tanto para una aplicación particular tal conocimiento debe ser complementado con herramientas y tecnologías de soporte que competen al alumno investigar su aplicación.

2. Diego. F., & Christian C. (2012) "Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos", Para optar el título

profesional de Ingeniero de computación y sistemas, Universidad San Martin de Porres, determina como problemática principal que Card Perú no cuenta con los controles, medidas, procedimientos de seguridad necesarios para resguardar sus activos de información, tales como documentos, software, dispositivos físicos, personas, imagen, reputación y servicios, están expuestos altos niveles de riesgos, frente a las diversas amenazas físicas y lógicas existentes como son desastres naturales, estructurales, hardware, software, Red LAN y WAN, información, riesgo contra el patrimonio y otros riesgos.

El objetivo general que se presenta en esta investigación es reducir y mitigar los riesgos de los activos de información de los procesos que se encuentra bajo la gerencia de tecnología de Card Perú que ponen en peligro los recursos, servicios y continuidad de los procesos tecnológicos. Es una investigación experimental y se llega a las siguientes conclusiones que el implementar una política de seguridad y que los colaboradores la conozcan es de vital importancia para la empresa.

3. Talavera Álvarez, V.R. (2013). Tesis: *Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013.* Tesis para optar por el Título de Ingeniero Informático, PUCP.

Conclusiones:

Existe una brecha importante en cuanto a seguridad de la información en la institución sobre la que se ha realizado el presente proyecto. La principal falencia que debería ser resuelta cuanto antes es involucrar a la dirección en las acciones del plan que se debe definir con motivo de la implementación del SGSI institucional, el cual debería ser gestionado como un proyecto institucional, de manera que se cuente con el apoyo de las distintas direcciones y áreas del INMP. Es de vital importancia

que se defina formalmente el comité de Seguridad de la Información, órgano que debería encargarse del proyecto de implementación del SGSI y que deberá contar con el apoyo de la Dirección General de modo que se facilite el acceso a la información de todas las áreas pertinentes. El factor humano que constituyen los colaboradores debe ser apropiadamente atacado en cuanto a los cambios que el proyecto. Esto deberá incluir sesiones de capacitación en las que se concientice al personal sobre la importancia de la información con la cual se realizan las labores institucionales, así como fomentar el cumplimiento de las políticas que garantice la seguridad de la misma. Es probable que la implantación de las nuevas condiciones de empleo para los colaboradores antiguos sea recibida con rechazo dado que muchos de ellos se encuentran trabajando mucho tiempo en la institución y puedan percibir este cambio como una amenaza. Este posible obstáculo deberá ser debidamente manejado en conjunto con el área de recursos humanos. El tipo de actividades que realiza a la institución, así como la normativa a la cual se encuentra sujeta en cuanto a la gestión de Historias Clínicas (MINSA, 2005), obliga a que la información recolectada de los pacientes o generada durante la atención sea almacenada en formato físico. Este escenario al cual se adiciona la falta de definición de los procesos de negocio y la caótica presencia de personas externas a la institución – pacientes, familiares, estudiantes, entre otros – incrementa la probabilidad de pérdida o extracción de información. Es pertinente indicar que las medidas actuales de aseguramiento de estos documentos no cumplen con los mínimos necesarios tanto en acceso físico, como en protección frente a incidentes como incendios, inundaciones, daño por humedad, etc. Esto ha sido evidenciado en paralelo al presente trabajo en el Censo Nacional de Archivos Realizado el presente año (ARCHIVO GENERAL DE LA NACIÓN, 2014). El SGSI se encuentra

estrechamente relacionado con la gestión de riesgos de una institución y tal como se puede evidenciar en el presente documento, el análisis que realiza no está sesgado a los activos o controles tecnológicos que la institución pueda tener o requiera.

2.2 Bases teóricas

2.2.1 Sistema de gestión de seguridad de la información (SGSI)

Un Sistema de Gestión de Seguridad de Información es un conjunto de responsabilidades, procesos, procedimientos y recursos que establece la alta dirección con el propósito de dirigir y controlar la seguridad de los activos de información y asegurar la continuidad de la operatividad de la empresa (ISO 17799:2005; Alexander, 2007). Un SGSI está soportado en cuatro grandes y continuas etapas para su mantención en el tiempo, las cuales son:

Figura Nº 01: Etapas de SGSI

2.2.1.1 Seguridad de Información

"Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma". [1]

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos saber que puede ser confidencial. Puede ser divulgada, mal utilizada, robada, borrada, saboteada, etc. La información es poder, y según las posibilidades estratégicas que ofrece tener a acceso a cierta información, ésta se clasifica como:

- **Crítica**: Es indispensable para la operación de la empresa.
- **Valiosa**: Es un activo de la empresa y muy valioso.
- **Sensible**: Debe ser conocida por las personas autorizadas

Los términos de seguridad de la información, seguridad informática y garantía de la información son usados frecuentemente como sinónimos porque todos ellos persiguen una misma finalidad al proteger la confidencialidad, integridad y disponibilidad de la información.

2.2.1.2 Activo de Información

Según Alexander (2007, 44) "Un activo es algo que tiene valor o utilidad para la organización, sus operaciones comerciales y su continuidad. Por esta razón, los activos necesitan tener protección para asegurar una correcta operación del

[1] Fuente: Definición que se tomó como referencia del siguiente enlace: http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

negocio y una continuidad en las operaciones. Para cualquier tipo de empresa son de vital importancia la gestión y la responsabilidad por los activos.

En este punto es importante clarificar que es un activo de información. Según el ISO 17799:2005 (Código de práctica para la gestión de seguridad de información), un activo de información es algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger. Los activos de información se pueden clasificar en las siguientes categorías:

- Activos de información (datos, manuales de usuario, etc.).
- Documentos de papel (contratos).
- Activos de software (aplicación, software de sistemas, etc.).
- Activos físicos (computadoras, medios magnéticos, etc.).
- Personal (clientes, empleados).
- Imagen de la compañía y reputación
- Servicios (comunicaciones, etc.)."

2.2.1.3 Confidencialidad

La confidencialidad es la propiedad para prevenir la divulgación de información a personas o sistemas no autorizados. Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y el comerciante de una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte no autorizada obtiene

el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se publica información privada, cuando un laptop con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc

2.2.1.4 Integridad

Para la Seguridad de la Información, la integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, asimismo, hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital es uno de los pilares fundamentales de la seguridad de la información.

2.2.1.5 Disponibilidad

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar

funcionando correctamente. La alta disponibilidad en sistemas tiene como objetivo estar disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema

La disponibilidad además de ser importante en el proceso de seguridad de la información es, además variada en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requiera, tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de web, etc; mediante el uso de clusters o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar.

2.2.1.6 Vulnerabilidad

Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una organización.

Al tratar de definir las vulnerabilidades, la mejor manera es pensar en las debilidades del sistema de seguridad. Las vulnerabilidades no causan daño. Simplemente son condiciones que pueden hacer que una amenaza afecte un activo.

Las vulnerabilidades pueden clasificarse como:

- Seguridad de los recursos humanos (falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, falta de políticas para el uso correcto de las telecomunicaciones, no eliminar los accesos al término del contrato de trabajo, carencia de procedimientos que asegure la entrega de activos al término del contrato de trabajo, empleados desmotivados).

- Control de acceso (segregación inapropiada de redes, falta de política sobre escritorio y pantalla limpia, falta de protección al equipo de comunicación móvil, política incorrecta para el control de acceso, passwords sin modificarse).
- Seguridad física y ambiental (control de acceso físico inadecuado a oficinas, salones y edificios, ubicación en áreas sujeta a inundaciones, almacenes desprotegidos, carencia de programas para sustituir equipos, susceptibilidad de equipos a variaciones de voltaje).
- Gestión de operaciones y comunicaciones (complicadas interfaces para usuarios, control de cambio inadecuado, gestión de red inadecuada, carencia de mecanismos que aseguren el envío y recepción de mensajes, carencia de tareas segregadas, carencia de control de copiado, falta de protección en redes públicas de conexión).
- Mantenimiento, desarrollo y adquisición de sistemas de información (protección inapropiada de llaves criptográficas, políticas incompletas para el uso de criptografía, carencia de validación de datos procesados, carencia de ensayos de software, documentación pobre de software, mala selección de ensayo de datos).

2.2.1.7 Amenaza

En las organizaciones, los activos de información están sujetos a distintas formas de amenazas. Una amenaza puede causar un incidente no deseado, que puede generar daño a la organización y a sus activos.

Una amenaza es la indicación de un potencial evento no deseado. Esta definición hace referencia a una situación en la cual una persona pudiera hacer algo indeseable o una ocurrencia natural.

Para una empresa, las amenazas pueden ser de distintos tipos con base en su origen. Las amenazas se pueden clasificar en:

- Amenazas naturales (inundaciones, tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales).
- Amenazas a instalaciones (fuego, explosión, caída de energía, daño de agua, pérdida de acceso, fallas mecánicas).
- Amenazas humanas (huelgas, epidemias, materiales peligrosos, problemas de transporte, pérdida de personal clave).
- Amenazas tecnológicas (virus, hacking, pérdida de datos, fallas de hardware, fallas de software, fallas en la red, fallas en las líneas telefónicas).
- Amenazas operacionales (crisis financiera, pérdida de suplidores, fallas en equipos, aspectos regulatorios, mala publicidad).
- Amenazas sociales (motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo).

Como se nota las amenazas se pueden generar de fuentes o eventos accidentales o deliberados.

Para que una amenaza cause daño a un activo de información tendría que explotar una o más vulnerabilidades del sistema, aplicaciones o servicios usados por la organización a efectos de poder ser exitosa en su intención de hacer daño. (Alexander, 2007)

2.3 Definiciones conceptuales

a) Tecnología

Es el conjunto de conocimientos técnicos, científicamente ordenados, que permiten diseñar, crear bienes, servicios que facilitan la adaptación al medio ambiente y satisfacer tanto las necesidades esenciales como los deseos de la humanidad.

b) Cliente

Son aquellos o aquellas personas que llegan a una empresa a realizar una compra o que le brinden un servicio.

c) Calidad de servicio

Según Reyes, S; Mayo, J. y Loredo, N. (2009) "La calidad de servicio percibida por el cliente es entendida como un juicio global del consumidor que resulta de la comparación entre las expectativas sobre el servicio que van a recibir y las percepciones de la actuación de las organizaciones prestadoras del servicio" d) Servicio

Según Betancourt Y. y Mayo J (2010) "el termino servicio proviene del lation servitium y define a la acción y efecto de servir. También permite referirse a la prestación humana que satisface alguna necesidad social y que no consiste en la producción de bienes materiales".

d) Riesgo

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema.

Entre las amenazas, existen las vulnerabilidades, los riesgos y los activos de información, una secuencia de causalidad y probabilidad de ocurrencia.

Figura Nº 02: Elementos del riesgo

e. Riesgo residual

Es el riesgo remanente después de haber realizado el tratamiento del riesgo.

f. Control

Aquellos mecanismos y/o procedimientos que regulan el propio funcionamiento del SGSI.

g. International Organization for Standardization (ISO)

La Organización Internacional de Normalización o ISO nacida tras la Segunda Guerra Mundial (23 de febrero de 1947), es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su

función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

La ISO es una red de los institutos de normas nacionales de 162 países, sobre la base de un miembro por país, con una Secretaría Central en Ginebra (Suiza) que coordina el sistema. La Organización Internacional de Normalización (ISO), con sede en Ginebra, está compuesta por delegaciones gubernamentales y no gubernamentales subdivididos en una serie de subcomités encargados de desarrollar las guías que contribuirán al mejoramiento ambiental.

h. ISO/IEC 27002:2005

"Código de prácticas para la gestión de la seguridad de la

información". Es un modelo que da recomendaciones para las buenas prácticas. Es un modelo basado en el anexo A de la ISO/IEC 27001:2005, el cual amplía y explica de forma detalla cómo implantar los controles del anexo A de la ISO/IEC 27001:2005 Este método no puede utilizarse para la certificación. (Alexander, 2007)

i. Política de seguridad

Son las directrices y objetivos generales de una empresa relativos a la seguridad, expresados formalmente por la dirección general. La política de seguridad forma parte de la política general y debe ser aprobada por la alta dirección.

La Política de seguridad de una empresa es un documento

auditable ya sea por los auditores internos de la empresa o por externos en busca de una certificación, inclusive por el cliente. Por este motivo este documento

debe ser entendido a todos los niveles, desde el personal operativo / operador hasta los altos mandos (directores, gerentes, etc.).

Una política de seguridad es como la "carta de presentación de la empresa" donde se exponen los puntos que quiere dar a conocer la empresa, ¿a qué se dedica?, ¿qué quiere lograr?, ¿bajo qué método trabaja?, ¿Cómo lo quiere lograr? Estas cuatro preguntas son la estructura que debe llevar la carta de presentación ante el cliente, el quien al leer estos cuatro puntos va a tener una idea muy clara de la empresa a la que está a punto de comprar sus productos o servicios.

2.4 Formulación de la hipótesis

En la Investigación que corresponde a este Proyecto de tesis, No se Planteara ninguna hipótesis por el hecho de que su planteamiento de problema define un alcance Descriptivo, el cual a su vez no pretende Pronosticar ni Afirmar un Hecho.

CAPITULO III: METODOLOGIA

3.1 Diseño Metodológico

3.1.1 Tipo

Basado en un diseño no experimental, estudio intrínseco y holístico de un caso, que consiste en observar, tal como se da en su contexto natural y actual, el funcionamiento ya existente del sistema de gestión de seguridad de información para la municipalidad provincial de Huaral y en comprender todo el caso como una única unidad de análisis.

3.1.2 Nivel de Investigación

El nivel de la investigación es transversal descriptiva cuyo objetivo será recolectar datos acerca del sistema de gestión de seguridad de información para la municipalidad provincial de Huaral, que está teniendo lugar en el año 2017, para luego describirlo.

3.2 Población y Muestra

3.2.1 Población

La Presente investigación se aplicará a los Jefes de Área, Directivos, Administrativos y personal técnico del Centro de Cómputo de la Municipalidad Provincial de Huaral, en total suman 25 personas.

3.2.2 Muestra

La desagregaremos de la siguiente manera:

1º) Directivos y funcionarios: 10

2º) Personal de cómputo: 15

3.3 Operacionalización de Variables e Indicadores

Variables	Dimensiones	Indicador	Instrumento
SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN	Análisis y diseño Controles internos informáticos	X_1: Uso de clave confidencial X_2: Uso de técnicas de control X_3: Protección de datos en caso de accidente. X_4: Accesibilidad de los sistemas X_5: Protección de datos modificados X_6: Utilización de Sistemas por usuarios autorizados.	Encuesta Encuesta Encuesta

3.4 Técnicas e Instrumentos de Recolección de Datos

3.4.1 Técnica a emplear

Las técnicas para la obtención de la información que se necesita para el desarrollo de esta investigación serán:

- ✓ Observación.
- ✓ Análisis documental
- ✓ Entrevista
- ✓ Encuestas

3.4.2 Descripción de los Instrumentos

Observación: Se aplica para observar todo lo relacionado con la utilización del plan de seguridad y salud en el trabajo, que permita evaluar el cumplimiento de las funciones, operaciones y procedimientos.

Análisis Documental: Con la finalidad de obtener un fundamento del problema de investigación para el presente trabajo de estudio, se revisará las fuentes escritas (textos, tesis, etc.) vinculadas al tema de estudio.

Entrevista: Se entrevistará a profesionales, técnicos y obreros quienes tienen a cabo la conducción de la Obra en mención.

Encuesta: Se elaborará un cuestionario de preguntas tipo Likert

3.5 Técnicas para el procesamiento de la información

A. Estadística descriptiva

Se encarga de describir a los sujetos estudiados en relación con todas y cada una de las variables recogidas.

B. Estadística inferencial

Se quiere estimar la asociación (si existe o no) entre 2 o más variables.

Proporcionará la teoría necesaria para inferir o estimar la toma de decisiones sobre la base de la información parcial mediante técnicas descriptivas. Se someterá a prueba:

- La hipótesis central
- Las hipótesis especificas

CAPITULO IV: SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA MUNICIPALIDAD PROVINCIAL DE HUARAL

4.1 Aspectos generales

A nivel metodológico es importante tener presente que el (MSPI) cuenta con una serie de guías anexas que ayudarán a las entidades a cumplir lo solicitado permitiendo abordar de manera detallada cada una de las fases del modelo, buscando a su vez comprender cuáles son los resultados a obtener y como desarrollarlos, incluyendo los nuevos lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano.

La implementación del Modelo de Seguridad y Privacidad de la Información, en la Entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

4.2 Metodología de gestión de riesgos (Alexander, 2007)

La metodología de gestión de riesgos mostrada a continuación es una recopilación de buenas prácticas para el análisis y evaluación de riesgos extraída del libro de Alexander, 2007.

A. Identificación de activos

Los activos de información en la empresa, dentro del alcance del SGSI, son fundamentales para una correcta implementación de un SGSI. El análisis y la evaluación del riesgo y las decisiones que se tomen en relación con el tratamiento

del riesgo en la empresa giran alrededor de los activos de información identificados.

Un activo es algo que tiene valor o utilidad para la organización, sus operaciones comerciales y su continuidad. Por esta razón, necesitan tener protección para asegurar una correcta operación del negocio y continuidad en sus operaciones. Para cualquier tipo de empresa son de vital importancia la gestión y la responsabilidad por los activos.

En este punto es importante clasificar los activos de información.

Estos se clasifican en las siguientes categorías:

- ✓ Activos de información (datos, manuales de usuario, etc.)
- ✓ Documentos de papel (contratos)
- ✓ Activos de software (aplicación, software de sistemas, etc.)
- ✓ Activos físicos (computadoras, medios magnéticos, etc.)
- ✓ Servicios (comunicaciones, etc.)

Como se aprecia, los activos de información son muy amplios. Es fundamental estar conceptualmente claros de qué es un activo de información y conocer sus distintas posibles modalidades, para así poder realizar un correcto análisis y una evaluación y, por ende, poder establecer adecuadamente el modelo ISO 27001:2005.

La metodología de las elipses (ver 3.1.3.2.4 B) desempeña un papel muy importante en esta etapa. Con base en las elipses, la empresa, considerando la categorización de los activos, debe iniciar la identificación de los activos de información.

En la organización, el proceso de identificación y tasación de activos debe realizarlo un grupo multidisciplinario compuesto por personas involucradas en los procesos y subprocesos que abarca el alcance del modelo. Es muy importante que los dueños de los activos principales conformen el grupo multidisciplinario. Como un "dueño de activos" se entiende aquella

persona que tiene una responsabilidad por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos, aprobada por la gerencia. Dentro del alcance del SGSI, los activos importantes deben identificarse con claridad, como ya se explicó, y posteriormente deben ser tasados para visualizar su impacto en la empresa por su deterioro o por sus fallas en: (1) confidencialidad, (2) integridad y (3) disponibilidad.

B. Identificación de requerimientos legales y comerciales relevantes para los activos identificados

- ✓ La primera fuente deriva de la evaluación de los riesgos que afectan a la organización. Aquí se determinan las amenazas de los activos, luego se ubican las vulnerabilidades, se evalúa su posibilidad de ocurrencia y se estiman los potenciales impactos.
- ✓ La segunda fuente es el aspecto legal. Aquí están los requerimientos contractuales que deben cumplirse.
- ✓ La tercera fuente es el conjunto particular de principios, objetivos y requerimientos para procesar información que la empresa ha desarrollado para apoyar sus operaciones.

4.3 Herramientas

A. Ciclo de Deming

El ciclo Deming es una herramienta de mejora continua. El ciclo consiste de una secuencia lógica de cuatro pasos repetidos que se deben de llevar a cabo consecutivamente. Estos pasos son:

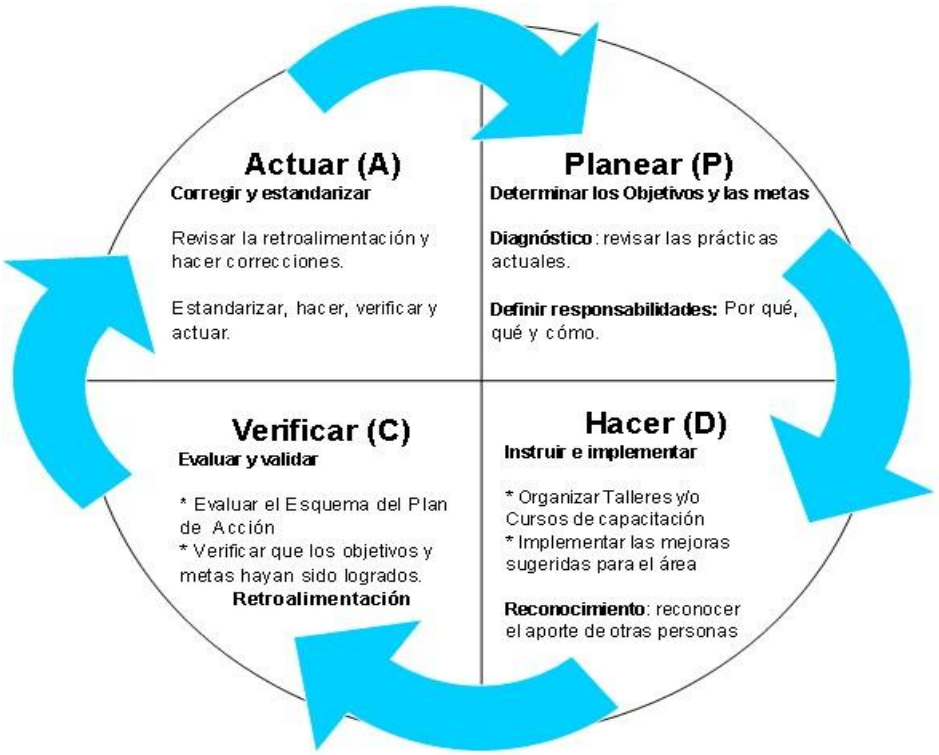

Figura Nº 03: Ciclo Deming

Los resultados de la implementación de este ciclo permiten a las empresas una mejora integral de la competitividad, de los productos y servicios, mejorando continuamente la calidad, reduciendo los costes, optimizando la productividad, reduciendo los precios, incrementando la participación del mercado y aumentando la rentabilidad de la empresa u organización.

B. ISO/IEC 27001:2005

La ISO 27001:2005 está orientada a establecer un sistema gerencial que permita minimizar el riesgo y proteger la información en las empresas, de amenazas externas o internas. La norma define a un Sistema de gestión de seguridad de información (SGSI) como:

"La parte del sistema de gestión global, basada en una orientación a riesgo de negocio, para establecer, implementar operar, monitorear, revisar, mantener y mejorar la seguridad de la información".

Es importante entender que la ISO/IEC 27001:2005 se ha desarrollado como modelo para el establecimiento, la implementación, la operación, el monitoreo, la revisión, el mantenimiento y la mejora de un SGSI para cualquier clase de organización. (Fuente www.slideshare.net)

C. ISO/IEC 27002:2005

"Código de prácticas para la gestión de la seguridad de la información". Es un modelo que da recomendaciones para las buenas prácticas. Es un modelo de la ISO/IEC 27001:2005, el cual amplia y explica de forma detalla como implantar los controles del anexo A de la ISO/IEC 27001:2005, este método no puede utilizarse para la certificación.

Figura Nº 04: Dominios de la ISO/IEC 27002:2005

D. Diagrama de flujo BPMN

Es una notación gráfica que describe la lógica de los pasos de un proceso de negocio. Esta notación ha sido especialmente diseñada para coordinar la secuencia de los procesos y los mensajes que fluyen entre los participantes de las diferentes actividades, la cual consta de las siguientes características:

- Es un estándar internacional de modelado de procesos.
- Independiente de cualquier metodología de modelado de procesos.
- Crea un puente estandarizado para disminuir la brecha entre los procesos de la organización y la implementación de éstos.
- Permite modelar los procesos de manera unificada y estandarizada permitiendo un entendimiento a todas las personas de la organización.

E. Gestión de proyectos – PMBOK

La dirección de proyectos es la aplicación de conocimientos, habilidades, herramientas y técnicas a las actividades de un proyecto para satisfacer los requisitos del proyecto. La dirección de proyectos se logra mediante la aplicación e integración de los procesos de dirección de proyectos de inicio, planificación, ejecución, seguimiento y control, y cierre. El director del proyecto es la persona responsable de alcanzar los objetivos del proyecto.

La dirección de un proyecto incluye:

- ✓ Identificar los requisitos
- ✓ Establecer unos objetivos claros y posibles de realizar
- ✓ Equilibrar las demandas concurrentes de calidad, alcance, tiempo y costes
- ✓ Adaptar las especificaciones, los planes y el enfoque a las diversas inquietudes y expectativas de los diferentes interesados.

Los directores del proyecto a menudo hablan de una "triple restricción" - alcance, tiempos y costes del proyecto - a la hora de gestionar los requisitos concurrentes de un proyecto. La calidad del proyecto se ve afectada por el equilibrio de estos tres factores. Los proyectos de alta calidad entregan el producto, servicio o resultado requerido con el alcance solicitado, puntualmente y dentro del presupuesto. La relación entre estos tres factores es tal que si cambia cualquiera de ellos, se ve afectado por lo menos otro de los factores. Los directores de proyectos también gestionan los proyectos en respuesta a la incertidumbre. El

riesgo de un proyecto es un evento o condición inciertos que, si ocurre, tiene un efecto positivo o negativo al menos en uno de los objetivos de dicho proyecto.

El equipo de dirección del proyecto tiene una responsabilidad profesional ante sus interesados, incluidos los clientes, la organización ejecutante y el público. Los miembros de PMI acatan un "Código de Ética", y quienes tienen la certificación de Profesional de la Dirección de Proyectos acatan un "Código de Conducta Profesional".

4.4 Metodologías

Se utilizó como metodología la gestión de riesgos, una metodología elaborada por el grupo del proyecto basada en el MAGERIT y en la metodología de gestión de riesgos encontrada en el libro de Alexander, 2007.

4.4.1 Metodología para el Diseño del SGSI (MEDIS)

La siguiente es una metodología desarrollada como referencias a la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) y la metodología de análisis y gestión de riesgos presentada en el libro de Alexander, 2007.

A) Política de SGSI

La Política de SGSI es una declaración de la Gerencia

que se define teniendo en consideración:

- Debe incluir el marco referencial para establecer los objetivos.
- Debe tomar en cuenta los requerimientos comerciales, legales, reguladores, y las obligaciones de la seguridad contractual,

- Debe estar alineada con el contexto de la gestión del riesgo estratégico de la gerencia,
- Debe establecer el criterio con el que se evalúa el riesgo,
- Debe ser revisada y aprobada por la gerencia.

B) Manual del SGSI

Para la elaboración del manual se debe tener en consideración lo siguiente:

- El manual del SGSI debe proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI.
- Se debe definir el alcance aplicable,
- Se debe definir responsabilidades de cumplimiento y ejecución.

C) Análisis de brechas

El análisis de brechas se debe elaborar, comparando el estado actual de la organización con los requisitos obligatorios indicados en la Circular N° G-140 de la SBS.

Para dicho análisis se debe realizar un estudio a los procesos actuales de la organización, donde se incluirá el porcentaje de cumplimiento para cada dominio obligatorio de la Circular N° G-140, siguiendo el siguiente formato:

Ítem	Requisitos Circular G-140	Cumple	Nivel Cumplimiento
Generalidades			
Seguridad lógica			
Seguridad de personal			
Seguridad física ambiental			
Inventario de activos y clasificación de la información			
Administración de las operaciones y comunicaciones			
Adquisición, desarrollo y mantenimiento de sistemas informáticos			
Procedimientos de respaldo			
Gestión de incidentes de seguridad de información			

Tabla Nº 01: Análisis de brechas

D) Análisis y evaluación de riesgos

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

(1) Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.

(2) Determinar a qué amenazas están expuestos aquellos activos.

(3) Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.

(4) Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

(5) Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Con el objeto de organizar la presentación, se tratan primero los pasos 1, 2, 4 y 5, obviando el paso 3, de forma que las estimaciones de impacto y riesgo sean “potenciales”: caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas del paso 3, derivando estimaciones realistas de impacto y riesgo.

La siguiente figura recoge este primer recorrido, cuyos pasos se detallan en las siguientes secciones:

Figura Nº 05: Elementos del riesgo

a) Identificación de procesos

Como primer paso se deben identificar todos los procesos que se encuentran dentro del alcance del SGSI y representarlos con diferentes herramientas; tales como: procedimientos, instructivos, caracterización, fichas, cartillas, etc.

Diagrama de procesos

b) Identificación de activos

Para la identificación de los activos se utiliza el método de las elipses. Esta metodología permite, con gran precisión, poder identificar los activos de información.

Lo primero que se debe hacer es determinar en la elipse concéntrica, los distintos procesos y subprocesos que están incluidos dentro del alcance del SGSI. A cada proceso se le identificaron sus respectivos subprocesos.

El segundo paso consiste en identificar en la elipse intermedia las distintas interacciones que los procesos de la elipse concéntrica tienen las diferentes áreas de la organización. Seguidamente, en la elipse externa, se identifican aquellas organizaciones extrínsecas a la empresa que tienen cierto tipo de interacción con los procesos y subprocesos identificados en la elipse concéntrica.

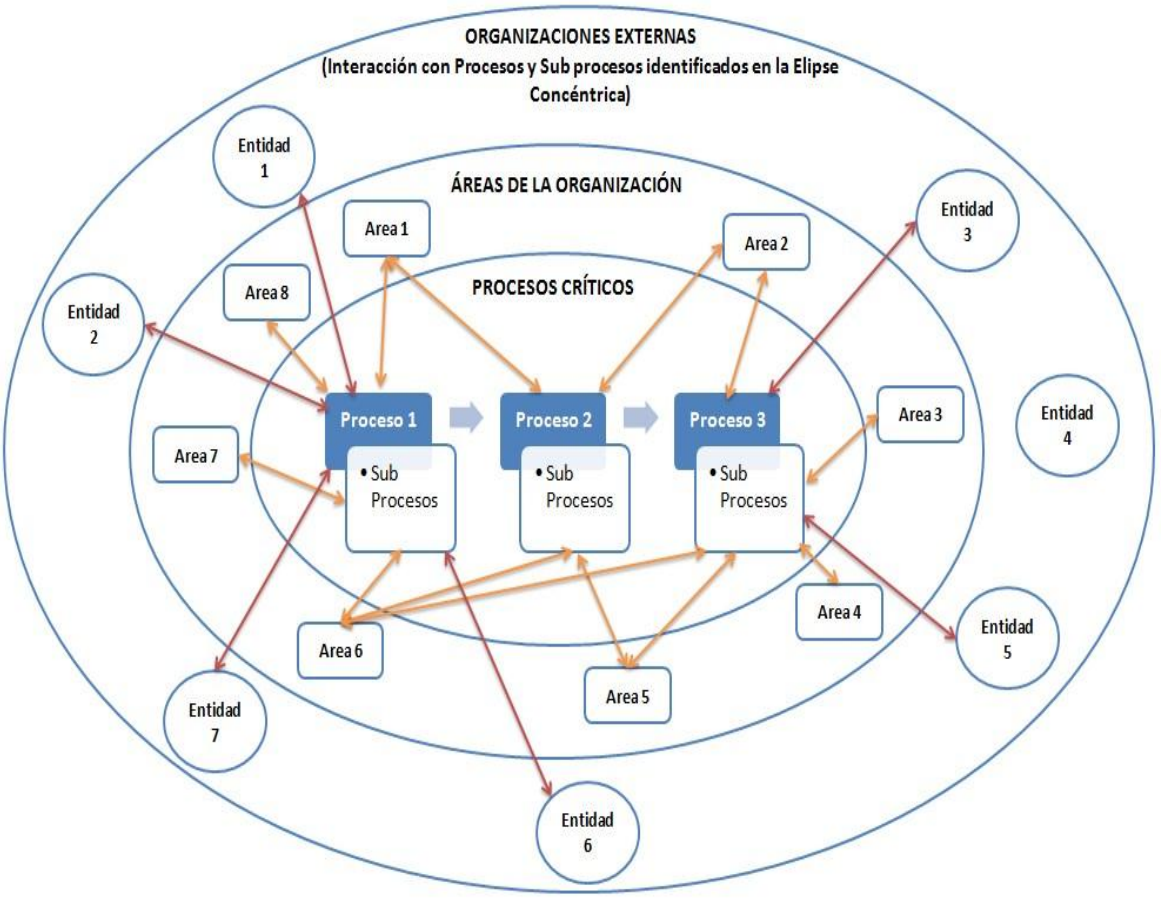

Figura Nº 06: Método de las elipses

El método de las elipses se utiliza como fuente de inspiración para derivar, posteriormente, al **documento de análisis para la identificación activos de información**, ya que, al analizar los procesos identificados y el flujo de información con las áreas y las entidades extrínsecas, se procede a identificar todos los activos de información que serán representados en el **documento inventario de activos de seguridad de información.**

Identificación de activos (elipses)

c) Inventario de activos

Para la elaboración del **documento inventario de activos de seguridad de información**, se debe tener en consideración lo siguiente, para la categorización de los Activos de Información:

CATEGORÍA DE ACTIVOS			
TIPO	**CÒDIGO**	**CATEGORÌA**	**EJEMPLO**
ACTIVOS DE INFORMACIÒN	I1	Información electronica	Base de datos y documentos creados y o conservados en medios electrónicos (correo electrónico, audio, video, entre otros).
	I2	Información escrita	Documentos creados y o conservados en papel.
	I3	Información hablada	Conversaciones presenciales, telefónicas, presentaciones orales o a través de medios virtuales (video conferencia).
	I4	Otro tipo de información	
ACTIVOS DE SOFTWARE	SW1	Software base o sistema operativo	Software Base o Sistema Operativo Windows 2000, Windows XP, Windows 2000 server, Windows 2003 server, Linux, Unix, etc.
	SW2	Software commercial o herramientas, utilitarios	Office, Adobe, Primo, entre otros.
	SW3	Software desarrollado por terceros	SAP, JD Edwards, Oracle

	SW4	Software desarrollado internamente	Sistema Integrado, Aplicativo, Modulo de Sistema, etc
	SW5	Software administración Base de Datos	SQL, Oracle, DB/2, Informix, etc.
	SW6	Otro software	
ACTIVOS DE HARDWARE	F1	Equipo procesamiento	Servidores, computadoras, laptops, entre otros.
	F2	Equipo comunicaciones	Routers, centrales digitales, máquinas de fax, entre otros.
	F3	Medio de almacenamiento	Discos, cintas, disquetes, CD‘s, DVD’s, memorias USB, entre otros.
	F4	Mobiliario y equipamiento	Estantes, cajas fuertes, archivadores, entre otros.
	F5	Otros equipos	Impresoras, fotocopiadoras, scanners, entre otros
SERVICIOS TERCEROS	S1	Procesamiento y comunicaciones	Servicio de Procesamiento de la información, de impression, de fotocopiadoras, de mensajería, telefonía fija y celular, entre otros.
	S2	Servicios generales	Calefacción, energía eléctrica, aire acondicionado, entre otros.
	S3	Otros servicios	Servicio de intermediación laboral, entre otros.

Tabla Nº 02: Inventario de activos

Para todos los activos de información deben existir siempre:

- **Usuario:** Rol que emplea el activo de información para su trabajo.
- **Responsable:** Rol que es dueño del activo de información.
- **Custodio: Rol** que custodia los activos de información.

Todos los activos de información inventariados deben tener ser valorizados según el siguiente cuadro:

d) Análisis y evaluación de riesgos

*** Identificación de amenazas**

Las amenazas son "cosas que ocurren". Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos de información y causar un daño. Una amenaza puede causar un incidente no deseado que puede generar daño a la organización y sus activos.

Para una empresa, las amenazas pueden ser de distintos tipos con base en su origen.

* **Clasificación de amenazas o Amenazas naturales** (inundaciones, sismos, incendios, tormentas, etc)

- Amenazas a instalaciones (energía, explosión, fuego, fallas, etc)
- Amenazas humanas (transporte, renuncias, huelgas, accidentes, etc)
- Amenazas tecnológicas (virus, hacking, red, fallas software hardware)
- Amenazas operacionales (crisis, legal, fallas equipos, proveedores)
- Amenazas sociales (motines, protestas, vandalismo, violencia, etc)

Inventario de activos

- **Identificación de amenazas y mecanismos de protección**

Una vez determinada que una amenaza puede perjudicar a un activo, hay que estimar si afecta a la confidencialidad, integridad y disponibilidad del SGSI.

La organización puede contar con mecanismos de protección los cuales reducen la probabilidad de ocurrencia de dichas amenazas. Se deben identificar los mecanismos de protección actual clasificada en: o **Preventivos**: Mecanismo de protección que previene a que la amenaza se materialice.

- **Detectivos**: Mecanismo de protección que detecta cuando una amenaza se materializa.
- **Correctivos**: Mecanismo de protección que ejecutará después que la amenaza se haya materializado.

*** Identificación de vulnerabilidades**

Las vulnerabilidades son debilidades de seguridad asociadas a los activos de información de una organización.

Al tratar de definir las vulnerabilidades, la mejor manera es pensar en las debilidades del sistema de seguridad. Las vulnerabilidades no causan daño. Simplemente son condiciones que pueden hacer que una amenaza se materialice y afecte un activo.

Es bueno entender que las vulnerabilidades y las amenazas deben presentarse juntas, para poder causar incidentes que pudiesen dañar los activos. Por esta razón es necesario entender la relación entre amenazas y vulnerabilidades. La pregunta fundamental es ¿Qué amenaza pudiese explotar cuál de las vulnerabilidades?

* **Clasificación de vulnerabilidades**

o Seguridad lógica

o Seguridad de recursos humanos

o Seguridad física y ambiental

o Seguridad gestión de operaciones y comunicaciones

o Mantenimiento, desarrollo y adquisición de sistemas de información

*** Determinación del impacto / probabilidad [2]**

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

El impacto mide el daño causado por un incidente en el supuesto de que ocurriera.

La frecuencia pone en perspectiva aquel impacto, pues una amenaza puede ser de terribles consecuencias pero de muy improbable materialización;

[2] Fuente: Cuadros elaborados por el grupo de proyecto para asignarle valores de ocurrencia y como afecta al negocio que una amenaza se materialice sobre un activo de información.

mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acumular un daño considerable.

Tomando en consideración las amenazas, mecanismos de protección actuales y las vulnerabilidades del sistema de seguridad para todos los activos de información se debe definir:

- La **valoración** de los activos, que es la sumatoria del impacto del activo en la **confidencialidad**, **integridad** y **disponibilidad** del SGSI, en una escala del 1(Muy Bajo) al 5 (Muy Alto).
- La **probabilidad** que las amenazas se materialicen, usando la siguiente clasificación:

5: Muy Alto	Ocurrencia diaria
4: Alto	Ocurrencia semanal
3: Medio	Ocurrencia mensual
2: Bajo	Ocurrencia anual
1: Muy bajo	Ocurrencia en dos años a más

Tabla Nº 03: Probabilidad de materialización de amenazas

- **Impacto** que ocasionaría el que las amenazas se materialicen, usando la siguiente clasificación:

5: Muy Alto	- Afecta a los socios - Afecta a los establecimientos - Afecta a los partners - Afecta a entidades regulatorias
4: Alto	- Afecta a más de un área de la empresa
3: Medio	- Afecta a un usuario, no hay posibilidad de trabajo alterno
2: Bajo	- Afecta a un usuario, existe posibilidad de trabajo alterno
1: Muy bajo	- No afecta a la productividad

Tabla Nº 04: Impacto que ocasiona una amenaza al materializarse

*** Determinación del riesgo**

El objetivo del análisis del riesgo es identificar y calcular los riesgos basados en la identificación de los activos, y en el cálculo de las amenazas y vulnerabilidades.

Los riesgos se calculan de la combinación de los valores de los activos, que expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad y del cálculo de la probabilidad de que amenazas y vulnerabilidades relacionadas se junten y causen un incidente.

Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia. El riesgo crece con el impacto y con la frecuencia.

Valoración = C + I + D

Riesgo = Probabilidad * Impacto + Valoración

Los riesgos no se pueden eliminar, solo mitigar, es por ello que se establece un nivel de tolerancia de riesgos, expresado en:

Totalmente Tolerable: TT	**4 – 15**
Regularmente Tolerable: RT	**16 – 25**
No Tolerable: NT	**26 – 40**

Para activos que tienen **mínimo** un riesgo que resulte **regularmente tolerable** o **no tolerable** se debe re-definir salvaguardas.

Los riesgos que resulten Totalmente Tolerable, son opcionales para ser tratados.

Análisis y evaluación de riesgos

e) Gestión del riesgo

*** Definición de salvaguardas**

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se evitan simplemente organizándose adecuadamente, otras requieren elementos técnicos, otra seguridad física y por último, están las políticas de personal.

Las salvaguardas se caracterizan por su eficacia frente al riesgo que pretenden mitigar. La salvaguarda ideal es 100% eficaz, lo que implica que:

- Es teóricamente idónea o Está perfectamente desplegada, configurada y mantenida o Se emplea siempre o Existen procedimientos claros de uso normal y en caso de incidencias
- Los usuarios están formados y concientizados o Existen controles que avisan de posibles fallos.

Las estrategias para el tratamiento de las salvaguardas pueden ser:

- **Reducción del riesgo (R):** Para todos aquellos riesgos donde la opción de reducirlos se ha tomado, se deben implementar controles apropiados para poder reducirlos a un nivel aceptable.
- **Aceptar el riesgo (A):** Muchas veces se presentan situaciones en la cual la organización no encuentra controles para mitigar el riesgo, o en la cual la implantación de controles tiene un costo mayor que las consecuencias del riesgo. En estas circunstancias, la decisión de aceptar el riesgo y vivir con las consecuencias es la más adecuada.

- **Transferencia del riesgo (T):** La transferencia del riesgo es una opción cuando para la compañía es difícil reducir o controlar el riesgo a un nivel aceptable. La alternativa de transferencia a una tercera parte es más económica ante estas circunstancias.
- **Evitar el riesgo (E):** Es cualquier acción orientada a cambiar las actividades, o la manera de desempeñar una actividad en particular, para así evitar la presencia del riesgo.
- Por cualquiera de las estrategias que se opte, todas las salvaguardas incurren en un costo y tiempo que estarán gestionados por el/los responsables de implementación.
- Para dimensionar el **costo aproximado** de la implantación de la salvaguarda elegida, se considera:

3	Alto costo
2	Medio costo
1	Bajo costo
D	Desconocido

- Para dimensionar el **tiempo aproximado** de la implantación de la salvaguarda elegida, se considera:

C	Corto plazo (Menos de 1 meses)
M	Mediano plazo (De 1 a 2 meses)
L	Largo plazo (Más de 3 meses)
D	Desconocido

*** Determinación del riesgo residual**

Si se han hecho todos los deberes a la perfección, el riesgo residual debe ser despreciable.

Si hay deberes a medio hacer (normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no controlan) entonces se dice que el sistema permanece sometido a un riesgo residual.

El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, se repiten los cálculos de riesgo usando el impacto residual y la nueva tasa de ocurrencia.

Riesgo Residual = Probabilidad R. * Impacto R. + Valoración

Totalmente tolerable: TT	**4 – 15**
Regularmente tolerable: RT	**16 – 25**
No tolerable: NT	**26 – 40**

Cuadro 3: Medición del impacto y probabilidad del riesgo [3]

Para los riesgos que resulten nuevamente r**egularmente tolerable** o **no tolerable** se debe re-definir nuevamente salvaguardas.

Los riesgos que resulten **totalmente tolerables**, son considerados **riesgos despreciables**, y no requieren más acciones, que el monitoreo periódico.

Tratamiento de riesgos

E) Plan de tratamiento de riesgos

La organización debe:

- Formular el plan de tratamiento de riesgo que identifique las acciones apropiadas, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información.

[3] Elaboración: los autores

- Implementar el plan de tratamiento de riesgos para poder lograr los objetivos, los cuales incluyen tener en consideración el financiamiento y asignación de roles y responsabilidades.

Plan de tratamiento de riesgos

CAPITULO V: VALIDACION DE INSTRUMENTOS Y RESULTADOS ESTADISTICOS

5.1 Validación de Instrumento

La selección de los instrumentos se realizó durante la operacionalización de variables; en ese momento se identificaron las dos variables; luego, se desagregaron en dimensiones, después estos en indicadores; posteriormente, se determinaron la cantidad de los ítems y finalmente se elaboraron los instrumentos, de acuerdo los indicadores. La selección de los instrumentos se hizo en razón a la intención de la investigación y de la validez que tenga.

El primer instrumento que se seleccionó corresponde a la variable: SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN. La validación del instrumento se realizó con los docentes expertos en investigación de la Universidad Nacional José Faustino Sánchez Carrión. Se elaboró los instrumentos de investigación, los cuales contiene 07 ítems. La validación de los instrumentos de recolección de datos se realizó a través de los siguientes procedimientos: Validez de contenido.

Sabino, Carlos (1992, pág. 154), con respecto a la Validez, sostiene: "Para que una escala pueda considerarse como capaz de aportar información objetiva debe reunir los siguientes requisitos básicos: validez y confiabilidad".

De lo expuesto en el párrafo anterior, se define la validación de los instrumentos como la determinación de la capacidad de las encuestas para medir las cualidades para lo cual fueron construidos.

A los referidos expertos se les entregó la matriz de consistencia, los instrumentos y la ficha de validación donde se determinaron: Sobre la base del procedimiento de validación descrita, los expertos consideraron que son pertinentes la existencia de una estrecha relación entre los criterios y objetivos del estudio y los ítems constitutivos del instrumento de recopilación de la información.

A. Método de expertos

La validez del instrumento (Instrumento para la toma de datos) de la presente investigación, se realizó por medio del juicio de expertos, en donde ellos evaluaron y a criterio propio calificaron el contenido del cuestionario empleado. Los expertos que realizaron fueron los siguientes:

Tabla Nº 05: Validez de contenido: Instrumento-cuestionario

JUECES EXPERTOS	**GRADO**	**NOMBRE**	**CIP N**
EXPERTO 1	INGENIERO	Ramírez Sánchez Julio Américo	144859
EXPERTO 2	INGENIERO	Gallardo Andrés Jhonar Ángel	138158
EXPERTO 3	INGENIERO	Soto La Rosa, José German	29081

El cálculo del Coeficiente de Validez del instrumento se realizó usando el método Delphi.

Las calificaciones para los criterios de validación, que se mencionan en la hoja de juicio de experto (Juicio de Expertos) con respecto al contenido del instrumento, se muestra en la siguiente tabla:

Tabla Nº 06: Calificación de los Expertos

N° PREGUNTA Y LTERNATIVAS	**EXPERTOS**			**Punt.**
	E1	**E2**	**E3**	
Pregunta N° 1 y sus alternativas	1	1	0	**2**
Pregunta N° 2 y sus alternativas	1	1	1	**3**
Pregunta N° 3 y sus alternativas	1	0	1	**2**
Pregunta N° 4 y sus alternativas	1	1	1	**3**
Pregunta N° 5 y sus alternativas	1	1	1	**3**
Pregunta N° 6 y sus alternativas	1	1	1	**3**
Pregunta N° 7 y sus alternativas	1	1	0	**2**
Puntaje total				**18**

Dónde: 1 = Totalmente de Acuerdo (TA)
0 = Totalmente en Desacuerdo (TD)

CÁLCULO DEL COEFICIENTE DE VALIDEZ:

$$Validez = \frac{Total\ de\ Acuerdo}{Total\ de\ Acuerdo\ (TA) + Total\ de\ Desacuerdo\ (TD)}$$

$$Validez = \frac{18}{18+3} = 0{,}86 = 86\%$$

Con una validez general de **86%** según la escala de validez el instrumento tiene MUY ALTA validez; (Ver Tabla 02), de acuerdo al criterio de los expertos.

Tabla Nº 07: Calificación de los Expertos

ESCALA	INDICADOR
0.01 – 0.20	Muy baja validez
0.21 – 0.40	Validez baja
0.41 – 0.60	Moderada validez
0.61 – 0.80	Alta validez
0.81 – 1.00	Muy alta validez

B. Confiabilidad

El criterio de fiabilidad del instrumento, se determinó en la presente investigación, por el coeficiente de Alfa de Crombach en prueba piloto, aplicada a los instrumentos para determinar la fiabilidad conformada por 7 ítems cuyas escalas tienen como respuesta cinco alternativas.

El Alfa de Crombach se trata de un índice de consistencia interna que toma valores entre 0 y 1 y que sirve para comprobar si el instrumento que se está evaluando recopila información defectuosa y por tanto nos llevaría a conclusiones equivocadas o si se trata de un instrumento fiable que hace mediciones estables y consistentes.

Tabla Nº 08: Interpretación del Coeficiente de Confiabilidad

Rangos	*Magnitud*
0,81 a 1,00	Muy alta
0,61 a 0,80	Alta
0.41 a 0,60	Moderada
0,21 a 0,40	Baja
0,01 a 0.20	Muy baja

El análisis de fiabilidad de la prueba de Alfa de CromBach del instrumento, se realizó con el apoyo del programa estadístico SPSS versión 23; obteniendo el siguiente resultado:

Tabla Nº 09: Procesamiento de los casos

		N	%
Casos	Válido	6	87,51
	Excluido[a]	1	12,49
	Total	7	100,0

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

Tabla Nº 10: Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
0,862	07

Interpretación:

Se aprecia que el valor del coeficiente de Alfa de Cronbach es de **0.862**, lo cual permite decir que el cuestionario es su versión 07 ítems tiene una **Muy alta** fiabilidad.

Como el instrumento presenta una muy alta fiabilidad, podemos afirmar que existen razones suficientes para indicar que el instrumento es aplicable.

5.2 Análisis y resultados estadísticos

Se procesaron los datos recolectados de los resultados del cuestionario.

Ítem 1: ¿En la Municipalidad se produce lo que es un análisis de riesgo?

Tabla Nº 11: En la Municipalidad se produce lo que es un análisis de riesgo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	18	72,0	72,0	72,0
	Completamente de acuerdo	5	20,0	20,0	92,0
	No sabe/no opina	2	8.0	8,0	100.0
Total		25	100,0		

Interpretación:

En la Tabla 7, que corresponde al ítem 1, se puede observar que del 100%, 25 personas encuestados, el 72.0% refieren estar de acuerdo, el 20.0% está muy de acuerdo y el 8,0% No sabe/no opina.

Ítem 2: ¿Cree Ud. que es necesario tomar medidas de protección de seguridad en la Municipalidad?

Tabla Nº 12: Cree Ud. que es necesario tomar medidas de protección de seguridad en la Municipalidad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	17	68,0	68,0	68,0
	Completamente de acuerdo	7	28,0	28,0	96,0
	No sabe/no opina	1	4,0	4,0	100.0
Total		25	100,0		

Interpretación:

En la Tabla 8, que corresponde al ítem 2, se puede observar que del 100%, 25 personas encuestados, el 68.0% refieren estar de acuerdo, el 28.0% está muy de acuerdo y el 4,0% No sabe/no opina.

Ítem 3: ¿Considera relevante la seguridad de la información de la Municipalidad?

Tabla Nº 13: Considera relevante la seguridad de la información de la Municipalidad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	20	80,0	80,0	80,0
	Completamente de acuerdo	04	16,0	16,0	96,0
	No sabe/no opina	1	4,0	4,0	100.0
Total		25	100,0		

Interpretación:

En la Tabla 9, que corresponde al ítem 3, se puede observar que del 100%, 25 personas encuestados, el 80.0% refieren estar de acuerdo, el 16.0% está muy de acuerdo y el 4,0% No sabe/no opina.

Ítem 4: ¿Se utiliza una copia de seguridad o backup cuando se pierde una determinada cantidad de archivos?

Tabla Nº 14: Se utiliza una copia de seguridad o backup cuando se pierde una determinada cantidad de archivos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	20	80,0	80,0	80,0
	Completamente de acuerdo	03	12,0	12,0	92,0
	No sabe/no opina	02	8,0	8,0	100.0
Total		25	100,0		

Interpretación:

En la Tabla 10, que corresponde al ítem 4, se puede observar que del 100%, 25 personas encuestados, el 80.0% refieren estar de acuerdo, el 12.0% está muy de acuerdo y el 8,0% No sabe/no opina.

Ítem 5: ¿Cree Ud. que la restricción de acceso a programas y archivos maliciosos pueden proteger tu equipo de cómputo?

Tabla Nº15: Cree Ud. que la restricción de acceso a programas y archivos maliciosos pueden proteger tu equipo de cómputo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	15	60,0	60,0	60,0
	Completamente de acuerdo	5	20.0	20,0	80,0
	No sabe/no opina	5	20,0	20,0	100.0
Total		25	100,0		

Interpretación:

En la Tabla 11, que corresponde al ítem 5, se puede observar que del 100%, 25 personas encuestados, el 60.0% refieren estar de acuerdo, el 20.0% está muy de acuerdo y el 20,0% No sabe/no opina.

Ítem 6: ¿Es necesario para mantener la seguridad física el uso de sistema de aire acondicionado en el área de cómputo?

Tabla Nº 16: Es necesario para mantener la seguridad física el uso de sistema de aire acondicionado en el área de cómputo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	17	68,0	68,0	68,0
	Completamente de acuerdo	05	20,0	20,0	88,0
	No sabe/no opina	3	8,0	12,0	100.0
Total		25	100,0		

Interpretación:

En la Tabla 12, que corresponde al ítem 6, se puede observar que del 100%, 25 personas encuestados, el 68.0% refieren estar de acuerdo, el 20.0% está muy de acuerdo y el 12,0% No sabe/no opina.

Ítem 7: ¿Para que el usuario tenga confianza de que sus datos estén protegidos es necesario tener un plan de Seguridad Informática en la Municipalidad?

Tabla Nº 17: Para que el usuario tenga confianza de que sus datos estén protegidos es necesario tener un plan de Seguridad Informática en la Municipalidad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	15	60,0	60,0	60,0
	Completamente de acuerdo	08	32,0	32,0	92,0
	No sabe/no opina	2	8,0	8,0	100.0
Total		25	100,0		

Interpretación:

En la Tabla 13, que corresponde al ítem 7, se puede observar que del 100%, 25 personas encuestados, el 60.0% refieren estar de acuerdo, el 32.0% está muy de acuerdo y el 8,0% No sabe/no opina.

CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

1. Se concluye, Establecer la relación entre sistema de gestión de seguridad de información y las diversas amenazas físicas y lógicas existentes en la Municipalidad Provincial de Huaral, a fin de cautelar la información y no estén expuestas a diversas formas de amenazas.

2. Un sistema de información surge para satisfacer las necesidades de información y comunicación de un grupo de personas. Su misión es promover que el saber que reside en cualquier lugar de una organización, se distribuya de forma conveniente a otros individuos y pase a ser un activo de la empresa. - El sistema debe, además, poseer la capacidad de "crecer", no es necesario que sea "grande" desde el principio; lo esencial es que "crezca" con el tiempo adaptándose al medio y a las necesidades de la organización.

3. Es de vital importancia que se defina formalmente el comité de Seguridad de la Información, órgano que debería encargarse del proyecto de implementación del SGSI y que deberá contar con el apoyo de la Administración de la Municipalidad, de modo que se facilite el acceso a la información de todas las áreas pertinentes. El factor humano que constituyen los colaboradores debe ser apropiadamente atacado en cuanto a los cambios del proyecto. Esto deberá incluir sesiones de capacitación en las que se concientice al personal sobre la importancia de la información con la cual se realizan las labores institucionales, así como fomentar el cumplimiento de las políticas que garantice la seguridad de la misma. Es probable que la implementación de las nuevas condiciones de empleo para los colaboradores antiguos sea recibida con rechazo dado que muchos de ellos se encuentran trabajando mucho tiempo en la institución y puedan percibir este cambio como una amenaza. Este posible obstáculo deberá ser debidamente manejado en conjunto con el área de recursos humanos.

4. La seguridad informática es el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.

5. Uno de las posibles consecuencias de una intrusión es la pérdida de datos. Es un hecho frecuente y ocasiona muchos trastornos, sobre todo si no estamos al día de las copias de seguridad. Y aunque estemos al día, no siempre es posible recuperar la totalidad de los datos.

6. Otro de los problemas más dañinos es el robo de información sensible y confidencial. La divulgación de la información que posee la municipalidad sobre sus clientes puede acarrear demandas millonarias contra esta. Con la constante evolución de las computadoras es fundamental saber que recursos necesitar para obtener seguridad en los sistemas de información.

6.2 Recomendaciones

Implementar la propuesta de SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA MUNICIPALIDAD PROVINCIAL DE HUARAL**,** con el cual se asegura la seguridad de los activos y la confiabilidad de la información.

CAPITULO VII: FUENTES DE INFORMACION

7.1 Fuentes bibliográficas

Alvarez Basaldúa, L. D. (2005). Seguridad en Informática- Auditoría en Sistemas. *Tesis de Maestría*. México: Universidad Iberoamericana . Obtenido de http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

Cervantes Sánchez, O., & Ochoa Ovalle, S. (Julio de 2012). Seguridad Informática. (Edumed.net, Ed.) Obtenido de www.eumed.net/rev/cccss/21/

Córdova Rodríguez, N. E. (2013). Plan de Seguridad Informática para una Entidad Financiera. *Tesis de Pregrado*. Perú: Universidad Nacional Mayor de San Marcos.

Gómez, L., & Andrés, A. (2009). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. *Iso 27001*. España

Hermoso, R., & Vasirani, M. (2012). Seguridad Informática y Control de Acceso. *Tesis de Pregrado*. España: Universidad Rey Juan Carlos.

Juárez Vargas, H. (2005). Sistema de Seguridad de Software Aplicando Criptografía. *Tesis de pregrado*. Perú: Universidad Nacional del Altiplano. Obtenido de http://www.unap.edu.pe

Stolk, A. (2013). Técnicas de Seguridad Informática con software libre. México. Obtenido de http://www.human.ula.ve/ceaa/temporal/fundamentos de
seguridad.pdf

Tallana Farinango, L. (2012). Auditoría de Seguridad Informática de la Empresa Corporación Elite. *Tesis de pregrado*. Ecuador: Universidad de las Américas Laureate Internacional Universities.

Viteri Jiménez, M. J. (2014). Políticas de Seguridad Informática en el Departamento de Tecnología de la Información y Comunicación. *Tesis de pregrado*. Ecuador: Universidad Técnica Estatal de Quevedo. Obtenido de http://repositorio.uteq.edu.ec/handle/43000/130

ANEXOS

Anexo 1: Juicio de expertos

Anexo 2: Matriz de Consistencia

Anexo 3: Cuestionario

1. Juicio de expertos

JUICIO DE EXPERTOS 1.A

I. DATOS GENERALES

1.1. Apellidos y nombres del juez: ……

1.2. Especialidad: ……Grado: ……

1.3. Nombre del instrumento evaluado: Encuesta

1.4. Autor del instrumento:

II. DATOS DE LA INVESTIGACIÓN

2.1 Título: SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA MUNICIPALIDAD PROVINCIAL DE HUARAL

2.2 Objetivo: Reducir y mitigar los riesgos de los activos de información de los procesos del Sistema de Gestión de Seguridad de Información para la Municipalidad Provincial de Huaral.

III. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	Nunca	Algunas Veces	Casi Siempre	Siempre
		1	2	3	4
OBJETIVIDAD	Permite medir hechos observables				
CLARIDAD	Está formulado con un lenguaje apropiado y comprensible				
COHERENCIA	Tener relación entre las variables				
ORGANIZACIÓN	Presentación ordenada: problema–objetivos–hipótesis				
ACTUALIDAD	Adecuado al avance de la ciencia y tecnología para el desarrollo.				
PERTINENCIA	Permite conseguir datos de acuerdo a los objetivos planteados y correspondientes				
SUFICIENCIA	Comprende aspectos de la variable en Calidad y cantidad suficiente en el proceso				
CONSISTENCIA	Pretende conseguir datos basados en Teorías o modelos teóricos				

IV. CALIFICACIÓN

N	INTERVALO	INTERPRETACION
1	[0.01-0.20>	Muy baja
2	[0.21-0.64>	Baja
3	[0.41-0.69>	Moderada
4	[0.61-0.80>	Alta
5	[0.81-0.94]	Muy alta

Huacho, Octubre 2017

……..

JUICIO DE EXPERTOS 1.B

I. DATOS GENERALES

1.1. Apellidos y nombres del juez: …….
1.2. Especialidad: ……Grado: …….
1.3. Nombre del instrumento evaluado: Encuesta
1.4. Autor del instrumento:

II. DATOS DE LA INVESTIGACIÓN

2.1 Título: SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA MUNICIPALIDAD PROVINCIAL DE HUARAL

2.2 Objetivo: Reducir y mitigar los riesgos de los activos de información de los procesos del Sistema de Gestión de Seguridad de Información para la Municipalidad Provincial de Huaral.

III. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	Nunca	Algunas Veces	Casi Siempre	Siempre
		1	2	3	4
OBJETIVIDAD	Permite medir hechos observables				
CLARIDAD	Está formulado con un lenguaje apropiado y comprensible				
COHERENCIA	Tener relación entre las variables				
ORGANIZACIÓN	Presentación ordenada: problema–objetivos–hipótesis				
ACTUALIDAD	Adecuado al avance de la ciencia y tecnología para el desarrollo.				
PERTINENCIA	Permite conseguir datos de acuerdo a los objetivos planteados y correspondientes				
SUFICIENCIA	Comprende aspectos de la variable en Calidad y cantidad suficiente en el proceso				
CONSISTENCIA	Pretende conseguir datos basados en Teorías o modelos teóricos				

IV. CALIFICACIÓN

N	INTERVALO	INTERPRETACION
1	[0.01-0.20>	Muy baja
2	[0.21-0.64>	Baja
3	[0.41-0.69>	Moderada
4	[0.61-0.80>	Alta
5	[0.81-0.94]	Muy alta

Huacho, Octubre 2017

……..

JUICIO DE EXPERTOS 1.C

I. DATOS GENERALES

1.1. Apellidos y nombres del juez: …….
1.2. Especialidad: ……Grado: …….
1.3. Nombre del instrumento evaluado: Encuesta
1.4. Autor del instrumento:

II. DATOS DE LA INVESTIGACIÓN

2.1 Título: SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA MUNICIPALIDAD PROVINCIAL DE HUARAL

2.2 Objetivo: Reducir y mitigar los riesgos de los activos de información de los procesos del Sistema de Gestión de Seguridad de Información para la Municipalidad Provincial de Huaral.

III. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	Nunca	Algunas Veces	Casi Siempre	Siempre
		1	2	3	4
OBJETIVIDAD	Permite medir hechos observables				
CLARIDAD	Está formulado con un lenguaje apropiado y comprensible				
COHERENCIA	Tener relación entre las variables				
ORGANIZACIÓN	Presentación ordenada: problema–objetivos–hipótesis				
ACTUALIDAD	Adecuado al avance de la ciencia y tecnología para el desarrollo.				
PERTINENCIA	Permite conseguir datos de acuerdo a los objetivos planteados y correspondientes				
SUFICIENCIA	Comprende aspectos de la variable en Calidad y cantidad suficiente en el proceso				
CONSISTENCIA	Pretende conseguir datos basados en Teorías o modelos teóricos				

IV. CALIFICACIÓN

N	INTERVALO	INTERPRETACION
1	[0.01-0.20>	Muy baja
2	[0.21-0.64>	Baja
3	[0.41-0.69>	Moderada
4	[0.61-0.80>	Alta
5	[0.81-0.94]	Muy alta

Huacho, Octubre 2017

…….

ANEXO No 01: MATRIZ DE CONSISTENCIA
TEMA: SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA MUNICIPALIDAD PROVINCIAL DE HUARAL

Formulación del problema	Objetivos	Hipótesis	Variable	Indicadores	Instrumento
Problema general	**General**				
¿Qué relación existe entre el sistema de gestión de seguridad de información y las diversas amenazas físicas y lógicas existentes en la Municipalidad Provincial de Huaral?	Establecer la relación entre sistema de gestión de seguridad de información y las diversas amenazas físicas y lógicas existentes en la Municipalidad Provincial de Huaral.	En la Investigación que corresponde a este Proyecto de tesis, No se Planteara ninguna hipótesis por el hecho de que su planteamiento de problema define un alcance Descriptivo, el cual a su vez no pretende Pronosticar ni Afirmar un Hecho.	**Sistema de Gestión de Seguridad de Información**	X1: Uso de clave confidencial X2: Uso de técnicas de control X3: Protección de datos en caso de accidente.	ENCUESTA ENCUESTA
Problemas específicos	**Específicos**				
¿En qué medida los desastres naturales, estructurales, Hardware, Software y otros procedimientos de seguridad de información Influirían en un Deficiente sistema de gestión de seguridad de información para la Municipalidad Provincial de Huaral?	Implementar una Política de Seguridad de Información a fin de Reducir las diversas Amenazas físicas y lógicas existentes en la Municipalidad Provincial de Huaral.			X4: Accesibilidad de los sistemas X5: Protección de datos modificados	ENCUESTA ENCUESTA

¿En qué medida los altos niveles de riesgos, frente a las diversas amenazas físicas y lógicas Influirían en un Deficiente sistema de gestión de seguridad de información para la Municipali Provincial de Huaral?	Determinar cómo Monitorear de manera Eficiente los Incidentes y Vulnerabilidades de Seguridad de la Información para Reducirlos en la Municipalidad Provincial de Huaral.			X6: Utilización de Sistemas por usuarios autorizados.	ENCUESTA

ANEXO 03

Cuestionario de Encuesta

I. PRESENTACIÓN

Estimado (a) señor (a), el presente cuestionario es parte de una investigación que tiene por finalidad obtener información, acerca de la Recolección de datos para las Variables

II. INSTRUCCIONES

- Este cuestionario es anónimo. Por favor responda con sinceridad.
- Escriba a que área pertenece, lea detenidamente cada ítem. Responda el ítem y ponga una escala valorativa que se muestra en el cuadro.
- Gracias por su colaboración.

Área: _____

Escala valorativa

Siempre	Casi siempre	Algunas veces	Nunca
1	2	3	4

PREGUNTAS	Siempre	Casi Siempre	Algunas Veces	Nunca
1. ¿En la Municipalidad se produce lo que es un análisis de riesgo?				
2. ¿Cuándo es necesario tomar medidas de protección?				
3. ¿Considera relevante la seguridad de la información de la Municipalidad?				
4. ¿Se utiliza una copia de seguridad o backup cuando se pierde una determinada cantidad de archivos?				
5. ¿Cree Ud. que la restricción de acceso a programas y archivos maliciosos pueden proteger tu equipo de cómputo?				
6. ¿Es necesario para mantener la seguridad física el uso de sistema de aire acondicionado en el área de cómputo?				
7. ¿Para que el usuario tenga confianza de que sus datos estén protegidos es necesario tener un plan de Seguridad Informática en la Municipalidad?				

MIEMBROS DEL JURADO Y ASESOR

……

PRESIDENTE

Ing. Angel Huamán Tena

……

SECRETARIO

Ing. Máximo Darío Palomino Tiznado

…….

VOCAL

Ing. William Joel Marín Rodriguez

…….

ASESOR

Ing. Víctor Fredy Espezua Serrano