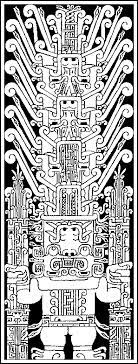
**UNIVERSIDAD NACIONAL FEDERICO VILLARREAL**

**FACULTAD DE INGENIERIA INDUSTRIAL Y DE SISTEMAS**

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

ESPECIALIDAD DE INGENIERIA DE SISTEMAS



PLAN DE TESIS

“METODOLOGÍA DE SEGURIDAD INFORMÁTICA BASADA EN ISO 27001 PARA MEJORAR LA INTEROPERABILIDAD ENTRE LAS INSTITUCIONES PÚBLICAS EN LA MUNICIPALIDAD PROVINCIAL DEL CALLAO.”

**AUTOR**

NOE FLAVIO CASTAÑEDA GAMA

LIMA – PERU

2021

Indice

[TÍTULO 5](#_Toc69160638)

[AUTOR 5](#_Toc69160639)

[LUGAR DONDE SE VA A REALIZAR LA INVESTIGACIÓN 5](#_Toc69160640)

[1 DESCRIPCIÓN DEL PROYECTO 5](#_Toc69160641)

[1.1 ANTECEDENTES 5](#_Toc69160642)

[1.2 PLANTEAMIENTO DEL PROBLEMA 12](#_Toc69160643)

[1.2.1 DESCRIPCIÓN DE LA PROBLEMÁTICA 12](#_Toc69160644)

[1.2.2 DESCRIPCIÓN DEL PROBLEMA 13](#_Toc69160645)

[1.2.3 FORMULACION DEL PROBLEMA 14](#_Toc69160646)

[1.2.3.1 PROBLEMA GENERAL 14](#_Toc69160647)

[1.2.3.2 PROBLEMA ESPECIFICO 14](#_Toc69160648)

[1.3 OBJETIVO 14](#_Toc69160649)

[1.3.1 OBJETIVO GENERAL 14](#_Toc69160650)

[1.3.2 OBJETIVO ESPECIFICO 14](#_Toc69160651)

[1.4 JUSTIFICACIÓN E IMPORTANCIA 15](#_Toc69160652)

[1.4.1 JUSTIFICACIÓN 15](#_Toc69160653)

[1.4.2 IMPORTANCIA 15](#_Toc69160654)

[1.5 ALCANCE Y LIMITACIONES 16](#_Toc69160655)

[1.5.1 ALCANCE 16](#_Toc69160656)

[1.5.2 LIMITACIONES 16](#_Toc69160657)

[1.5.2.1 DELIMITACIÓN ESPACIAL 16](#_Toc69160658)

[1.5.2.2 DELIMITACIÓN TEMPORAL 17](#_Toc69160659)

[2 MARCO TEORICO 17](#_Toc69160660)

[2.1 SISTEMA DE GESTION DE SEGURIDAD DE INFORMACION 17](#_Toc69160661)

[2.2 INFORMACION 18](#_Toc69160662)

[2.3 SEGURIDAD DE LA INFORMACION 18](#_Toc69160663)

[2.4 ISO 19](#_Toc69160664)

[2.5 ISO 27001 20](#_Toc69160665)

[2.6 ISO/IEC 27001:2013 Tecnología de Información. Técnicas de Seguridad. 22](#_Toc69160666)

[2.7 PDCA (Plan, Do, Check, Act) 22](#_Toc69160667)

[2.8 OCTAVE 24](#_Toc69160668)

[3 HIPOTESIS Y OPERALIZACION DE LAS VARIABLES 25](#_Toc69160669)

[3.1 HIPOTESIS GENERAL 25](#_Toc69160670)

[3.2 HIPOTESIS ESPECIFICAS 25](#_Toc69160671)

[3.3 VARIABLES 26](#_Toc69160672)

[3.3.1 VARIABLE INDEPENDIENTE 26](#_Toc69160673)

[3.3.2 VARIABLE INTERVINIENTE 26](#_Toc69160674)

[3.3.3 VARIABLE DEPENDIENTE 26](#_Toc69160675)

[3.3.4 OPERACIONALIDAD DE LAS VARIABLES 27](#_Toc69160676)

[3.4 TIPO 28](#_Toc69160677)

[3.5 POBLACION 28](#_Toc69160678)

[3.6 UNIVERSO SOCIAL 28](#_Toc69160679)

[3.7 MUESTRA 29](#_Toc69160680)

[4 METODO 29](#_Toc69160681)

[4.1 DISEÑO DE LA INVESTIGACION 29](#_Toc69160682)

[4.2 ESTRATEGIA DE PRUEBA DE HIPOTESIS 30](#_Toc69160683)

[4.3 TECNICA DE RECOLECCION DE DATOS 31](#_Toc69160684)

[4.3.1 INSTRUMENTOS DE RECOLECCION DE DATOS 31](#_Toc69160685)

[5 CRONOGRAMA 32](#_Toc69160686)

[6 PRESUPUESTO 33](#_Toc69160687)

[7 BIBLIOGRAFIA 34](#_Toc69160688)

[ANEXOS 35](#_Toc69160689)

[7.1 ANEXO A : MATRIZ DE CONSISTENCIA 35](#_Toc69160690)

[7.2 ANEXO B : DEFINICION DE TERMINOS 36](#_Toc69160691)

# TÍTULO

Metodología de seguridad informática basada en basada en ISO 27001, para mejorar la interoperabilidad entre las instituciones públicas para la Municipalidad Provincial del Callao.

# AUTOR

Noe Flavio Castañeda Gama

# LUGAR DONDE SE VA A REALIZAR LA INVESTIGACIÓN

Municipalidad Provincial del Callao – Jr. Paz Soldán #252 – Callao

# DESCRIPCIÓN DEL PROYECTO

# ANTECEDENTES

**Diana Elizabeth Tola Franco (2015 - Ecuador)** en su investigación sobre "IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA DE CONSULTORÍA Y AUDITORÍA, APLICANDO LA NORMA ISO/IEC 27001”, nos dice que es importante establecer los objetivos y políticas del sistema de gestión de seguridad de la información, ya que estos van delineando el camino hacia donde la organización desea dirigirse para preservar la confidencialidad, integridad y disponibilidad de la información y por lo tanto es relevante la participación de la alta gerencia.

Los sistemas de Gestión de Seguridad de Información bajo la norma ISO 27001, se basan en la prevención, por lo tanto, es muy importante identificar los riesgos a los que están expuestos los activos para así evitar pérdidas económicas u operacionales.

Una vez identificados los riesgos a los que están expuestos los activos de información, es necesario implementar controles, con la finalidad de proteger estos activos y lograr minimizar la probabilidad de que se materialicen los riesgos o el impacto que pueden tener sobre la organización.

Dentro del ciclo de un Sistema de Gestión de Seguridad de la Información, basado en ISO 27001, se encuentra la mejora continua lo cual hace que sea muy importante que la organización se asegure de crear procedimientos para el monitoreo y revisión del sistema, los mismos que deben cubrir incidentes de seguridad, auditorías internas y revisiones gerenciales. Estos elementos aportan retroalimentación al Sistema posibilitando conocer el estado del mismo y aplicar acciones correctivas, si fuera el caso, que permitan el cumplimiento de los planes y objetivos.

Conclusiones:

* Debido a que en las organizaciones es primordial la optimización de recursos, el establecimiento del alcance del sistema de gestión de seguridad de la información se convierte en una actividad muy importante ya que delimita el campo de acción y el uso de recursos.
* Es importante establecer los objetivos y políticas del sistema de gestión de seguridad de la información, ya que estos van delineando el camino hacia donde la organización desea dirigirse para preservar la confidencialidad, integridad y disponibilidad de la información y por lo tanto es relevante la participación de la alta gerencia.
* La adopción de la metodología MAGERIT para el análisis de riesgos, permitirá identificar de manera oportuna la probabilidad y el impacto de que se materialicen los riesgos y de esta manera poder establecer controles que nos ayuden a prevenirlos.

Recomendaciones:

* La concientización de la compañía es un pilar fundamental de esta norma, por lo cual la organización debe poner mucho empeño en despertar el interés y compromiso de todos sus empleados.
* Contar con personal clave dentro de la empresa y con las competencias exigidas por la Norma ISO 27001:2005 para evitar la contratación de consultorías externas, cuyo costo suele ser alto.
* La organización debe tratar de facilitar las tareas operativas del sistema SGSI, para lo cual necesita utilizar herramientas tecnológicas que automaticen ciertas tareas.

**Daniel Elías Santos Llanos (2016 - Perú)** en su investigación sobre ESTABLECIMIENTO, IMPLEMENTACIÓN, MANTENIMIENTO Y MEJORA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA ISO/IEC 27001:2013, PARA UNA EMPRESA DE CONSULTORÍA DE SOFTWARE, nos dice que la operación del SGSI beneficia a toda la organización, ya que muchas de las actividades y controles que gestiona tienen alcance general; sin embargo, muchos otros, de carácter más exhaustivo (gestión de riesgos, auditorías internas, revisión por la dirección, entre otros), están limitados estrictamente a un sub conjunto de los procesos de la organización: aquellos que han sido declarados dentro del alcance del SGSI.

Bajo esta premisa, el ideal de toda organización sería incluir dentro del alcance de su sistema a todos aquellos procesos críticos o sensibles respecto a la información que manejan. Sin embargo, la realidad muestra que en las organizaciones no siempre se cuenta con recursos para hacerlo. Se debe tomar en cuenta que la inclusión de cada proceso en el alcance implica para cada uno de ellos un esfuerzo adicional: horas de trabajo de su personal, recursos para la implementación de controles y para otras actividades del sistema.

Se recomienda que el alcance inicial del SGSI (primer ciclo de operación) sea asumido en base a la disponibilidad de recursos de la organización, entendiendo que es válido definir que el sistema inicie con solo algunos de los procesos críticos y planifique la incorporación de los faltantes en los siguientes ciclos de operación del sistema, apelando al principio de mejora continua. Esta decisión deberá ser tomada por la dirección de la organización, en el momento en que se apruebe el alcance del sistema.

Conclusión:

* Se concluye que para elaborar adecuadamente los componentes que permitan cumplir los requisitos del estándar 27001 deben considerarse aquellos estándares que, aunque no son referenciados, forman parte del dominio de algunos de los requisitos del SGSI.
* Se concluye que, como resultado de las exigencias del proyecto y sus interesados, se han podido elaborar propuestas innovadoras asociadas a la metodología de gestión de riesgos, la normalización de los planes del sistema y realizar la verificación integral de cumplimiento de los componentes requeridos como requisitos por la ISO/IEC 27001:2013.

Recomendaciones:

* Se recomienda que el alcance inicial del SGSI (primer ciclo de operación) sea asumido en base a la disponibilidad de recursos de la organización, entendiendo que es válido definir que el sistema inicie con solo algunos de los procesos críticos y planifique la incorporación de los faltantes en los siguientes ciclos de operación del sistema, apelando al principio de mejora continua. Esta decisión deberá ser tomada por la dirección de la organización, en el momento en que se apruebe el alcance del sistema.
* Se recomienda tomar argumentos de rentabilidad como un referente para proponer a la dirección de una organización las bondades de un SGSI y los beneficios que puede generarle. De manera que se pueda obtener su apoyo y recursos para la operación del sistema.
* Se recomienda considerar como tema para futuras investigaciones una metodología ágil para la creación y operación progresiva de un SGSI, que planifique las actividades en pequeños ciclos de operación, de manera que se pueda contar con un SGSI activo respecto a la mayoría de requisitos del estándar, desde los primeros meses de su creación.
* Se recomienda como tema futuro la creación de un sistema integrado de gestión que integre el estándar 27001 y el de algún otro sistema de gestión distinto, tomando como referente los componentes diseñados en la presente investigación. De esta manera será posible identificar qué componentes de un sistema de gestión de seguridad de información son adaptables o reutilizables respecto a otros estándares.
* Se recomienda, para futuros trabajos, la implementación de un software que automatice la operación de un SGSI. Como valor distintivo, además de la cobertura integral de los requisitos se debería contemplar un diseño que: defina roles segregados, cuenten con funcionalidades que eviten ingresos erróneos, cuente con un esquema de alerta de tareas pendientes, y permita que un usuario inexperto pueda, con una breve capacitación, asumir su rol dentro del SGSI.

**Iván Ricardo Narváez Barreiros (2013 - Ecuador)** en su propuesta Aplicación de la Norma ISO 27001 para la implementación de un SGSI en la Fiscalía General del Estado, nos dice que, en la actualidad, la información es el activo más valioso de cualquier compañía o institución. Sobre esta base se observa que, los gobiernos, entidades financieras, entidades de control, centros de salud, entidades gubernamentales, empresas privadas realizan esfuerzos para la automatización de sus procesos, a fin de obtener una mejor productividad y eficiencia, esto a su vez demanda y genera una gran cantidad de información, que puede ser confidencial (ya sea por el mandato de alguna normativa legal o por secretos de investigación o producción), abarcando desde la información administrativa interna como datos personales de sus empleados, productos, situación financiera, etc, hasta información de facturación, rastreo de paquetes, datos de clientes, etc.

El SGSI (Sisteme de Gestion de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

En otros términos, lo que busca un SGSI es asegurar de la manera más eficiente que la información disponga de confidencialidad, integridad y disponibilidad, considerando a la información como un activo importante en la empresa o institución, a la vez de gestionar los riesgos a la que esta pueda ser sometida.

Conclusiones:

* Mediante metodologías de evaluación de riesgos es factible realizar un análisis de la situación actual de cualquier organización, para el presente trabajo se usaron COSO y OCTAVE sin embargo existen otros procedimientos como la ISO/IEC 27005 o ISO/IEC 13335.
* La normativa del sector público ni la normativa administrativa interna no contempla planes claros relacionados con la seguridad de la información.
* No está presente el concepto de SGSI en la FGE, por cuanto recae en varios componentes las variables que inducen vulnerabilidad, iniciando por una falta de cultura de seguridad de información entre los empleados hasta la implementación de controles formales en el mismo tema.

Recomendaciones:

* Establecer formalmente en la institución un Comité de Seguridad de la Información, debido a que este es el responsable de aprobar y gestionar varios componentes fundamentales del SGSI.
* Se debe promover de manera más agresiva los procedimientos relacionados con seguridad de la información en todas las unidades administrativas y misionales de la Institución a fin de iniciar un proceso de certificación con menor impacto hacia los usuarios.
* Para el caso de MITIGACIÓN de riesgos es necesario establecer los controles necesarios para implementarlos lo más pronto posible, sea el caso de controles disuasivos o compensatorios de acuerdo al caso que sea necesario.
* En el caso de los APLAZAMIENTO de riegos, se deben establecer planes y cronogramas para solucionar los potenciales problemas que pueden ocasionar.
* En el caso de ACEPTACION de riesgos, documentar las características de estas vulnerabilidades para establecer un procedimiento para que cuando sea posible mediante inversión económica o nueva tecnología este pueda ser mitigado o gestionado.

# PLANTEAMIENTO DEL PROBLEMA

## 1.2.1 DESCRIPCIÓN DE LA PROBLEMÁTICA

A nivel gubernamental en 2008 empiezan las actividades de recomendaciones de uso de IPv6, y en 2011 se inaugura la plataforma de interoperabilidad de entidades públicas, alojada en el BCP.

El concepto de Interoperabilidad del Estado es una de las vigas maestras de la reforma que el Estado peruano necesita impulsar para mejorar su relación con los ciudadanos y para su propia eficiencia interna. Está referido en el Decreto Legislativo Nº 1246, que aprobó diversas medidas de simplificación administrativa, y consiste en la interconexión gratuita entre entidades públicas para poner a disposición, acceder o suministrar la información y las bases de datos actualizadas que ellas administren, recaben, sistematicen, creen o posean respecto de sus usuarios o administrados, para la tramitación de sus procedimientos administrativos y sus actos de administración interna.

Existe la necesidad de contar con una infraestructura capaz de soportar sistemas de misión crítica, manteniendo las aplicaciones disponibles y resguardadas durante las 24 horas. (7X24X365), la cual no se viene dando.

La Municipalidad del Callao como ente participante de la interoperabilidad entre las entidades acreditadas por el Indecopi, debe asegurar el envío de información con Firmas y Certificados Digitales, pero al no contar con las medidas de correspondientes, la seguridad de la información podría estar en riesgo.

En este momento la Oficina Nacional del Gobierno Electrónico e Informática (ONGEI) ha elaborado un proyecto de Decreto Supremo para hacer obligatorio que todas las entidades de la Administración Pública implementen “progresivamente el uso del protocolo IPv6 en sus recursos informáticos, según el caso y de acuerdo al Plan de Migración e implementación del protocolo IPv6 de su entidad”.

## DESCRIPCIÓN DEL PROBLEMA

La Municipalidad Provincial del Callao, actualmente no cuenta con una metodología de seguridad que le permita cumplir con los requerimientos que la Oficina Nacional del Gobierno Electrónico e Informática (ONGEI) exige a las entidades públicas, con la finalidad de dar cumplimiento al D.S. Nº 081-2017-PCM y se integren a la Plataforma Nacional de Interoperabilidad cuya infraestructura tecnología esta administrada por la secretaria del Gobierno Digital.

## 1.2.3 FORMULACION DEL PROBLEMA

### 1.2.3.1 PROBLEMA GENERAL

¿Cuál es el grado de mejora con la implementación de un Sistema de Gestión de la Seguridad de la Información en la Municipalidad Provincial del Callao?

### 1.2.3.2 PROBLEMA ESPECIFICO

* ¿De qué manera la propiedad de la información será accesible solo con la debida y comprobada autorización?
* ¿De qué manera la información permanecerá correcta y sin modificaciones, manteniendo sus datos exactamente tal como fueron generados, sin ser alterado por terceros?
* ¿De qué manera la información será accesible cuando sea requerida a través de los canales adecuados siguiendo los procesos correctos?

# 1.3 OBJETIVO

## 1.3.1 OBJETIVO GENERAL

Implementar una metodología de seguridad informática basado en la norma ISO 27001, para la Municipalidad Provincial del Callao.

## 1.3.2 OBJETIVO ESPECIFICO

* Implementar los procedimientos correspondientes orientados a la confidencialidad de la información.
* Implementar los procedimientos correspondientes orientados a la integridad de la información.
* Implementar los procedimientos correspondientes orientados a la disponibilidad de la información.

# 1.4 JUSTIFICACIÓN E IMPORTANCIA

## 1.4.1 JUSTIFICACIÓN

La presente investigación permitirá a la Municipalidad Provincial del Callao, alinearse con otras entidades publicas para dar cumplimiento al Decreto Legislativo 1246, que aprueba las diversas medidas de simplificación administrativa, que consisten en la interconexión gratuita entre entidades del estado a través de la incorporación a la plataforma de interoperabilidad para poner a disposición, acceder o suministrar la información actualizada que ellas administren, recaben, sistematicen, creen o posean respecto de sus usuarios o administrados, para la tramitación de sus procedimientos administrativos y sus actos de administración interna.

## 1.4.2 IMPORTANCIA

La implementación de una metodología de seguridad basada en ISO 27001 es importante en una entidad por que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. Hacer uso de una metodología de este tipo permite a cualquier tipo de organización la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

Hacer uso de estas metodologías no solo va a mejorar la imagen de la entidad, también va a permitir que la información este segura, se cumplan los acuerdos de confidencialidad y este preparada para futuros retos.

# 1.5 ALCANCE Y LIMITACIONES

## 1.5.1 ALCANCE

Este trabajo tiene como alcance implementar una metodología en seguridad informática aplicando normas basada en el ISO 27001 en la Municipalidad Provincial del Callao, para dar cumplimiento al Decreto Legislativo 1246 para la integración a la plataforma de interoperabilidad que propone el Estado Peruano.

La investigación se enfoca en la mejora de seguridad informática para la Municipalidad Provincial del Callao, Jr, Paz Soldan 252 – Callao.

## 1.5.2 LIMITACIONES

### 1.5.2.1 DELIMITACIÓN ESPACIAL

El área de trabajo de esta investigación está centrada en la Provincia Constitucional Del Callao. Dicha ubicación hace referencia donde está ubicada geográficamente la entidad objeto de este estudio.

### 1.5.2.2 DELIMITACIÓN TEMPORAL

Esta investigación toma como muestra el estado de la seguridad informática en la entidad en el año 2020.

# 2 MARCO TEORICO

Para la compresión del trabajo presentado, se deben tener en cuenta algunos conceptos importantes, los cuales se detallan en los siguientes numerales:

# 2.1 SISTEMA DE GESTION DE SEGURIDAD DE INFORMACION

Llamado también (SGSI) por sus iniciales, consiste en políticas, procedimientos, directrices, recursos asociados y actividades, gestionadas colectivamente por una organización, en la búsqueda de la protección de sus activos de información. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio. Se basa en la evaluación del riesgo y los niveles de aceptación del riesgo de la organización, diseñada para tratar y gestionar los riesgos de manera efectiva. Analizar requisitos para la protección de los activos de información aplicar los controles adecuados para garantizar su protección, según sea necesario, contribuye a la implementación exitosa de un SGSI.

# 2.2 INFORMACION

Es un activo que, al igual que otros activos de negocio importantes, es esencial para la misión de una organización y por lo tanto necesita ser protegida de forma adecuada. La información puede ser almacenada en muchas formas, incluyendo: forma digital (por ejemplo: archivos de datos almacenados en medios electrónicos u ópticos), forma material (por ejemplo: en el papel), así como la información no estructurada en la forma de conocimiento de los empleados. La información puede ser transmitida por diversos medios, incluyendo: mensajería, comunicación electrónica o verbal. Cualquiera que sea la forma que adopte la información o el medio por el cual sea transmitida, siempre se necesita una protección adecuada. En muchas organizaciones la información depende de la tecnología de la información y las comunicaciones. Esta tecnología es usualmente un elemento esencial en la organización y permite facilitar la creación, procesamiento, almacenamiento, transmisión, protección y destrucción de la información.

# 2.3 SEGURIDAD DE LA INFORMACION

La seguridad de información incluye tres dimensiones principales: la confidencialidad, disponibilidad e integridad. Consiste en la aplicación y gestión de medidas de seguridad apropiadas, lo que implica la consideración de una amplia gama de amenazas, con el fin de garantizar el éxito y continuidad del negocio, de manera sostenida, y la minimización de los impactos de los incidentes de seguridad de la información.

Esto se logra mediante la implementación de un conjunto aplicable de controles, seleccionados a través del proceso de gestión de riesgos y administrados utilizando un SGSI; incluye las políticas, procesos, procedimientos, estructuras organizacionales, software y hardware para proteger los activos de información identificados. Estos controles deben ser especificados, implementados, monitoreados, revisados y mejorados cuando necesario, para asegurar que se cumplen los objetivos específicos de seguridad de información y del negocio son logrados. Se espera que los controles de seguridad de la información relevantes se

integren a la perfección con los procesos de negocio de la organización.

# 2.4 ISO

ISO (Internacional Organization for Standardization) es la Organización Internacional de Normalización, cuya principal actividad es la elaboración de normas técnicas internacionales.

Las normas ISO contribuyen a que el desarrollo, la producción y el suministro de bienes y servicios sean más eficaces, seguros y transparentes. Gracias a estas normas, los intercambios comerciales entre países son más fáciles y justos. Proporcionan a los gobiernos un fundamento técnico para la legislación en materia de salud, seguridad y medio ambiente. También contribuyen a la transferencia de tecnología a los países en vías de desarrollo y, además, sirven para proteger a los consumidores y usuarios en general, ante cualquier problema surgido de un producto o servicio, haciéndoles la vida más sencilla.

# 2.5 ISO 27001

Desde 1901 y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution) es responsable de la publicación de importantes normas como: BS 5750 publicada en 1979, origen de ISO 9001; BS 7750 publicada en 1992, origen de ISO 14001. La norma BS 7799 de BSI apareció por primera vez en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente. Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000. En el 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión. En 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO con algunos cambios, como estándar ISO 27001. Al tiempo se revisó y actualizó ISO 17799. Esta última norma se renombró como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido, así como el año de publicación formal de la revisión.

Esta norma, está constituida por 8 cláusulas y Anexos, de los cuales la parte principal del sistema son desde la cláusula 4 a la 8 y el Anexo A. Las cláusulas indican los procedimientos que deben ser implementados, los documentos que deben ser elaborados y los registros que deben ser mantenidos dentro de la organización. El anexo A indica los controles y objetivos de control a implementar con el fin de ser salvaguardas, los mismos que se encuentran distribuidos en 11 dominios que son: A.5 Política de seguridad, A.6 Organización de la seguridad de la información, A.7 Gestión de activos, A.8 Seguridad de los recursos humanos, A.9 Seguridad física y ambiental, A.10 Gestión de las comunicaciones y operaciones, A.11 Control de acceso, A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información, A.13 Gestión de incidentes en seguridad de la información, A.14 Gestión de la continuidad del negocio y A.15 Cumplimiento.

Por lo tanto, ISO 27001, es un estándar que proporciona un modelo para establecer, implementar, utilizar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Se basa en un ciclo de vida PDCA (del inglés Plan-Do-Check-Act, cuyo significado en español es Planear, Hacer, Verificar y Actuar; o ciclo de Deming) de mejora continua, al igual que otros sistemas de gestión (ISO 9001 para calidad, ISO 14001 para medio ambiente, etc.).

Es un estándar certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo puede solicitar una auditoría externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001.

# 2.6 ISO/IEC 27001:2013 Tecnología de Información. Técnicas de Seguridad.

Sistemas de Gestión de Seguridad de Información. Requerimientos

Es la última versión del estándar que establece los requisitos para los sistemas de gestión de seguridad de información. Define los requerimientos necesarios para el adecuado establecimiento, implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI). Es un estándar certificable.

# 2.7 PDCA (Plan, Do, Check, Act)

Planificar, hacer, verificar y actuar, es una estrategia de mejora continua. Este modelo permite una efectiva organización y documentación, lo cual es requerido para este proceso.



PLANIFICAR

* + - Planificación de la gestión del servicio.
    - Definir el alcance del SGSI en la organización.
    - Identificar los activos de información y tasarlos.
    - Hacer el análisis y evaluación del riesgo.
    - Determinar opciones para el tratamiento del riesgo.
    - Definir los procesos.
    - Definir los recursos, equipamiento, presupuestos, herramientas.

HACER

* + - Implementar la gestión y provisión del servicio.
    - Elaborar el plan de tratamiento del riesgo, detallando las acciones que deben emprenderse para implantar las opciones de tratamiento del riesgo escogidas.

VERIFICAR

* + - Monitorear, medir y verificar.
    - Desarrollar procedimientos de monitoreo.
    - Revisar regularmente el SGSI.
    - Revisar objetivos y plan de gestión del servicio.
    - Auditar internamente el SGSI.

ACTUAR

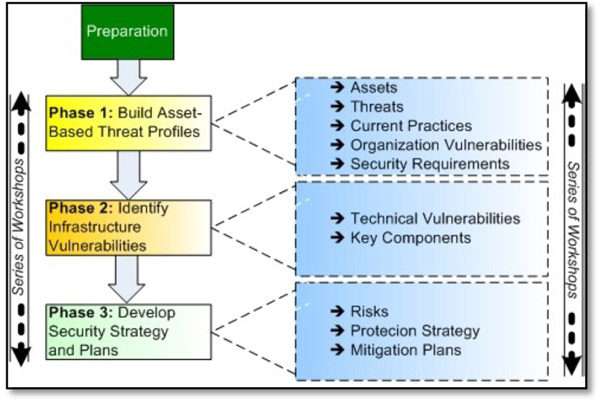
* + - Mantener el SGSI y desarrollar la mejora continua.
    - Identificar e implantar las mejoras.
    - Adoptar acciones correctivas y preventivas.
    - Verificar que las mejoras cumplen su objetivo.

# 2.8 OCTAVE

Operationally Critical Threat, Asset and Vulnerability Evaluation, es una metodología de análisis de riesgos desarrollada por la Universidad Carnegie Mellon en el año 2001, estudia los riesgos en base a tres principios, confidencialidad, integridad y disponibilidad.

Este modelo consta de 3 fases:

* + - La primera que es de evaluación de la entidad, se construyen los perfiles activo-amenaza, recogiendo los principales activos, así como las amenazas y requisitos como imperativos legales que puede afectar a los activos, las medidas de seguridad implantadas en los activos y las debilidades organizativas.
    - En la segunda se identifican las vulnerabilidades a nivel de infraestructura de TI.
    - En la última fase de desarrolla un plan y una estrategia de seguridad, siendo analizados los riesgos en esta fase en base al impacto que puede tener en la misión de la organización.



# 3 HIPOTESIS Y OPERALIZACION DE LAS VARIABLES

# 3.1 HIPOTESIS GENERAL

El desarrollo e implementación de una metodología de seguridad informática basada en ISO 27001, mejorará la seguridad de la información en la Municipalidad Provincial del Callao, para formar parte de la plataforma de interoperabilidad entre instituciones públicas.

# 3.2 HIPOTESIS ESPECIFICAS

H1: El desarrollo e implementación de procedimientos orientados a la confidencialidad de la información, mejoraran la seguridad de la información.

H2: El desarrollo e implementación de procedimientos orientados a la integridad de la información, mejoraran la seguridad de la información.

H3: El desarrollo e implementación de procedimientos orientados a la disponibilidad de la información, mejoraran la seguridad de la información.

# 3.3 VARIABLES

## 3.3.1 VARIABLE INDEPENDIENTE

- Seguridad de la Información.

## 3.3.2 VARIABLE INTERVINIENTE

- Metodología de seguridad de la información basada en ISO 27001.

## 3.3.3 VARIABLE DEPENDIENTE

- Interoperabilidad entre instituciones públicas del estado.

## 3.3.4 OPERACIONALIDAD DE LAS VARIABLES



# 3.4 TIPO

La investigación aplicada busca resolver problemas de la vida cotidiana y controlar situaciones prácticas. Se caracteriza por la aplicación, utilización y consecuencias practicas de los conocimientos. Este tipo de investigación busca el conocer para hacer, para actuar, para construir para modificar. En la presente investigación lo que se quiere es resolver la problemática referida a la Seguridad de la Información en la Municipalidad Provincial del Callao, aplicando un conjunto de normas que se encuentran contenidas en el ISO/IEC 27001. Por lo tanto, este trabajo debe ser considerado como tal.

# 3.5 POBLACION

La población es la Municipalidad Provincial del Callao, que se única en Jr. Paz Soldán #252 – Callao.

# 3.6 UNIVERSO SOCIAL

Profesionales: Ingenieros de Sistemas, Gerentes, Administradores, Técnicos.

Investigadores: Expertos en la industria, administración pública, distintas asociaciones de profesionales, centros de investigación o universidades.

# 3.7 MUESTRA

Relación de informes de incidencias que obra en el archivo de la Gerencia Informática de la Municipalidad Provincial Del Callao.

# 4 METODO

# 4.1 DISEÑO DE LA INVESTIGACION

1. **Identificación de procesos clave de la entidad**, el estándar ISO 27001 promueve la adopción de un enfoque de procesos para todas las fases del Sistema de Gestión de Seguridad de la Información, de tal modo que su aplicación servirá para la identificación y gestión sistemática de estas actividades y su interacción entre ellas. En tal sentido para alinearnos al estándar, la entidad deberá organizar sus actividades en procesos.
2. **Identificación de activos de información**, en este paso reconoceremos cuales son los activos que se encuentran asociados a los procesos de la organización. Cada proceso involucra activos de información especifica en sus diversos tipos y formatos.
3. **Elaboración de un diagnóstico**, en este paso procederemos a evaluar la situación actual de la entidad, respecto a los requisitos de la norma. Con este diagnóstico sabremos los mecanismos vigentes existentes que puedan ser aprovechados, así facilitar la implementación de ISO 27001.
4. **Planeamiento para la implementación del SGSI**, usaremos el modelo PDCA o también conocido como ciclo de mejora continua. Consta de 4 etapas cíclicas que nos van a permitir la disminución de fallos, aumento de la eficacia y eficiencia, solución de problemas, previsión y eliminación de riesgos potenciales.
5. **Gestión de riesgos**, para esta etapa usaremos la metodología OCTAVE, que estudia los riesgos en base a tres principios, confidencialidad integridad y disponibilidad, además de ser el que mas se ajusta a los objetivos que estamos buscando.

# 4.2 ESTRATEGIA DE PRUEBA DE HIPOTESIS

1. Recolección de Data

a. Determinar la información a recolectar y la fuente.

2. Proceso revisión

a. Verificar la calidad de la información.

3. Construcción

a. Cuantificar las incidencias mediante los indicadores.

4. Verificación y Análisis de resultados

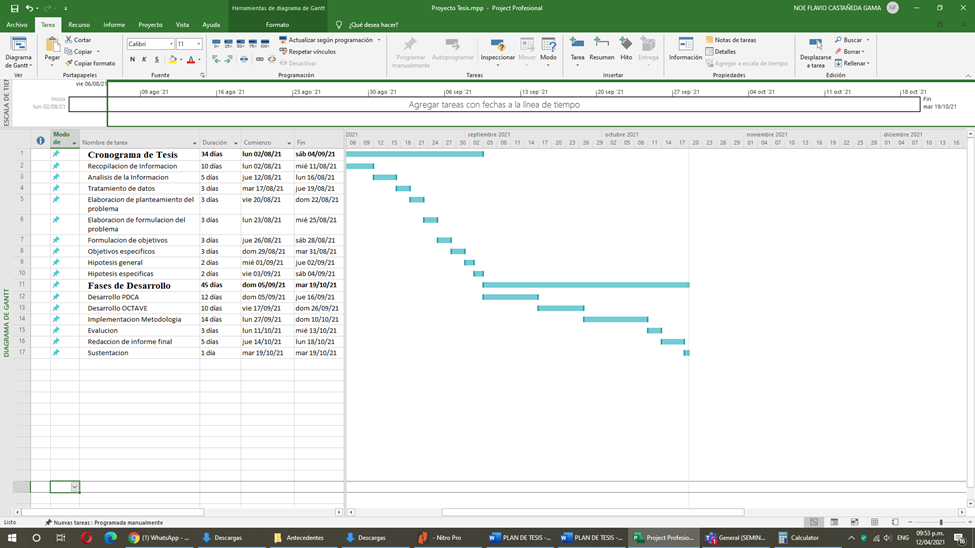
a. Comprobación del nivel de mejora con la implementación.

# 4.3 TECNICA DE RECOLECCION DE DATOS

## 4.3.1 INSTRUMENTOS DE RECOLECCION DE DATOS

Los datos serán obtenidos del archivo físico de informes de incidencias y del Sistema Help Desk.

# 5 CRONOGRAMA



# 6 PRESUPUESTO



# 7 BIBLIOGRAFIA

Lorena Mahecha Guzmán (2014) Sistema de Información para gestionar un SGSI basado en ISO 27001:2013

Luis Gómez Fernadandez, Pedro Pablo Fernández Rivero (2016) Como Implantar un Sgsi Según Iso/ iec 27001

Palmes, Paul C. (2010) PDCA - Un modelo para realizar auditorías internas.

Tobon Romero Yair, Zarate Aviña Jorge (2015) Análisis de Riesgos Metodología Octave

# ANEXOS

# 7.1 ANEXO A : MATRIZ DE CONSISTENCIA



# 7.2 ANEXO B : DEFINICION DE TERMINOS

**Sistema de Gestión**, un sistema de gestión utiliza un marco de recursos para lograr los objetivos de una organización. El sistema de gestión incluye la estructura organizativa, políticas, planificación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos.

**Confidencialidad**, propiedad de la limitación o restricción de la información a individuos, entidades o procesos no autorizados.

**Integridad,** propiedad de [la información de] exactitud y completitud.

**Disponibilidad**, propiedad de [la información de] ser accesible o usable cuando sea demandada por una entidad autorizada.

**Riesgo**, efecto que genera incertidumbre sobre [el logro de] los objetivos [de seguridad de información].

**Control**, medida que modifica la situación del riesgo.

**Vulnerabilidad**, debilidad de un activo o control que puede ser explotada por una o más amenazas.

**Amenaza**, causa potencial de un incidente inesperado, que podría resultar e daño a un sistema o a la organización.

**Consecuencia**, resultado de un evento, que afecta a los objetivos. Un evento puede llevar a un rango de consecuencias. Una consecuencia puede ser certera o incierta y en el contexto de la seguridad de información es usualmente negativa. Las consecuencias pueden ser expresadas de modo cualitativo o cuantitativo. Las consecuencias iniciales pueden escalar a través de efectos derivados.