UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Presentado por

YUVER HUAMÁN ANCCO

"MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON ISO/IEC 27001 PARA MINIMIZAR LA VULNERABILIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE SANTA MARÍA DE CHICMO, ANDAHUAYLAS 2018"

Asesor:

ING. ROBERTO QUISPE QUISPE

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

ANDAHUAYLAS – APURÍMAC – PERÚ

2018

Aprobación del Asesor

APROBACIÓN DEL ASESOR

Quién suscribe:

Ing. Roberto Quispe Quispe por la presente:

CERTIFICA,

Que, el Bachiller en Ingeniería de Sistemas, YUVER HUAMÁN ANCCO ha culminado satisfactoriamente el informe final de tesis intitulado: "MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON ISO/IEC 27001 PARA MINIMIZAR LA VULNERABILIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE SANTA MARÍA DE CHICMO, ANDAHUAYLAS 2018" para optar el Título Profesional de Ingeniero de Sistemas

Andahuaylas, 26 de junio del 2019.

Ing. Roberto Quispe Quispe
Asesor

Yuver Huamán Ancco
Tesista

Copia de acta de sustentación

Universidad Nacional José María Arguedas

Identidad y Excelencia para el Trabajo Productivo y el Desarrollo

FACULTAD DE INGENIERÍA

ACTA DE SUSTENTACIÓN DE TESIS

En la Av. José María Arguedas del Local Académico SL01 (Ccoyahuacho) en el auditorio de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional José María Arguedas ubicado en el distrito de San Jerónimo de la Provincia de Andahuaylas, siendo las 10:00 horas del día 23 de mayo del año 2019, se reunieron los docentes: Dr. Yalmar Temístocles Ponce Atencio, Dr. Julio César Huanca Marín, MSc. Richard Carrión Abollaneda, en condición de integrantes del Jurado Evaluador del Informe Final de Tesis intitulado: "MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON ISO/IEC 27001 PARA MINIMIZAR LA VULNERABILIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE SANTA MARÍA DE CHICMO – ANDAHUAYLAS 2018", cuyo autor es el Bachiller en Ingeniería de Sistemas **YUVER HUAMÁN ANCCO,** el asesor Ing. Roberto Quispe Quispe, con el propósito de proceder a la sustentación y defensa de dicha tesis.

Luego de la sustentación y defensa de la tesis, el Jurado Evaluador **ACORDÓ**: aprobar por unanimidad al Bachiller en Ingeniería de Sistemas **YUVER HUAMÁN ANCCO,** obteniendo la siguiente calificación y mención:

Nota escala vigesimal		Mención
Números	Letras	
13	trece	regular

En señal de conformidad, se procedió a la firma de la presente acta en 03 ejemplares.

.....
Dr. Yalmar Temístocles Ponce Atencio
Presidente del Jurado Evaluador

.....
Dr. Julio César Huanca Marín
Primer Miembro del Jurado Evaluador

.....
MSc. Richard Carrión Abollaneda
Segundo Miembro del Jurado Evaluador

Aprobación del Jurado Evaluador

APROBACIÓN DEL JURADO DICTAMINADOR

LA TESIS: MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON ISO/IEC 27001 PARA MINIMIZAR LA VULNERABILIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE SANTA MARÍA DE CHICMO, ANDAHUAYLAS 2018; para optar el Título Profesional de Ingeniero de Sistemas, ha sido evaluada por el Jurado Dictaminador conformado por:

PRESIDENTE: Dr. Yalmar Temistocles Ponce Atencio
PRIMER MIEMBRO: Dr. Julio César Huanca Marín
SEGUNDO MIEMBRO: MSc. Richard Carrión Abollaneda

Habiendo sido aprobado por UNANIMIDAD, en la ciudad de Andahuaylas el día 23 del mes de Mayo de 2019.

Andahuaylas, 26 de junio del 2019.

Dr. Yalmar Temistocles Ponce Atencio
Presidente del Jurado Evaluador

Dr. Julio César Huanca Marín
Primer Miembro del Jurado Evaluador

MSc. Richard Carrión Abollaneda
Segundo Miembro del Jurado Evaluador

Dedicatorias

En primer lugar doy gracias a DIOS, todo poderoso que me diste la oportunidad de vivir y de regalarme una familia maravillosa.

A mi adorada madre por haberme dado la vida y por ser parte fundamental de mi formación profesional, por darme sus valiosos consejos y por demostrarme que siempre podré contar con ella.

A mi padre por ser el pilar más importante, por demostrarme siempre su cariño y apoyo incondicional desde el primer momento para poder alcanzar un sueño más en la vida, por todo su tiempo y apoyo moral sobre todo por sus sabios conocimientos los mismos que fortalecieron mi sabiduría y potencializaron mis esfuerzos logrando así alcanzar el triunfo propuesto.

A mis hermanas por ser mi aliento y fortaleza para salir adelante, por compartir momentos significativos conmigo y por siempre estar dispuestas a escucharme y ayudarme en todo momento.

Agradecimiento

A Dios todo poderoso por darme la vida, su bendición y protegerme durante todo mi camino y darme fuerzas para compartir todos mis momentos con quienes más amo.

A mis padres por su esfuerzo, sacrificio y apoyo económico también apoyo moral para desarrollarme profesionalmente en la vida.

A mis hermanas y familiares por sus consejos brindados incondicionalmente en todos los momentos, por demostrarme que podemos ser grandes en la vida y por mi fortaleza cada nuevo día.

A mi asesor de tesis, Ing. Roberto Quispe Quispe, por su continuo apoyo a lo largo de esta investigación y no solo como docente si no como amigo, por su esfuerzo y dedicación brindándome sus conocimientos, su experiencia, paciencia, su motivación y su tiempo para así lograr los resultados de la investigación realizada.

A todos, mis amigos y compañeros por brindarme sus enseñanzas y ofrecerme su amistad a lo largo del tiempo que estuvimos albergados en las aulas de la MDSMC, nuestra alma mater.

A la Universidad Nacional José María Arguedas por la oportunidad que me brindó para convertirme profesional, gracias a cada maestro que hizo parte de este proceso integral de formación, que deja como producto terminado este grupo de graduados, como recuerdo y prueba viviente en la historia: esta tesis que perdurará dentro de los conocimientos y desarrollo de las demás generaciones que están por llegar.

Índice

Índice de Tablas

Índice de Gráficos

Resumen

La presente investigación tiene como objetivo principal la minimización de la vulnerabilidad de la información a la que está expuesta la Municipalidad Distrital de Santa María de Chicmo (MDSMC) por falta de aplicación de los controles de la seguridad de la información basadas en las buenas prácticas de la norma ISO/IEC 27001. Para cumplir los objetivos planteados se realizó diagnóstico de la seguridad de la información en los terminales tecnológicos y personal que maneja la información a través de preguntas referidas al tema, luego se implementó todos los controles seleccionados a través de capacitación al personal y trabajos en terminales informáticos para garantizar buen manejo de información importante que todo trabajador almacena en su terminal y así evitar que esté en peligro toda información vital ya sea físicos o lógicos. Este trabajo es de tipo cuantitativo ya que se hizo una encuesta para conocer la conciencia de la necesidad de seguridad por el personal que trabajan en las diferentes áreas con respecto a seguridad de la información. Los datos recolectados se analizó con el software spss v24 y los resultados obtenidos dan a conocer que la minimización de la vulnerabilidad de la información en la institución es satisfactorio, es necesario también implementar controles de seguridad de la información lo cual ayuda a fortalecer tres aspectos importantes, la confidencialidad, integridad y la disponibilidad de la información, pero los resultados también muestran la importancia del compromiso y trabajo en equipo que debe tener la MDSMC.

Palabras claves: Seguridad de la Información, ISO/IEC 27001, minimización de vulnerabilidad

Abstract

The main objective of this research is the minimization of the vulnerability of the information to which the district municipality of Santa María de Chicmo (MDSMC) is exposed due to the lack of application of the information security controls Based on the good practices of the ISO/IEC 27001 standard. In order to meet the objectives posed, it was carried out diagnosis of the security of the information in the technological terminals and personnel that manages the information by means of questions related to the subject, then it implemented all the controls selected through Staff training and computer terminal work to ensure good handling of important information that every worker stores in his/her terminal and thus prevent any vital information whether physical or logical. This work is quantitative as a survey was made to know the awareness of the need for security by staff working in different areas with respect to information security. The data collected was analyzed with the SPSS v24 software and the results obtained show that the minimization of the vulnerability of the information in the institution is satisfactory, it is also necessary to implement security controls of the information what Which helps to strengthen three important aspects, the confidentiality, integrity and availability of information, but the results also show the importance of commitment and teamwork that MDSMC should have.

Keywords: Information Security, ISO / IEC 27001, vulnerability minimization.

Chumasqa

Kay kunan watiqasqa kayna objetivoyuq qallariq hatun uchuyachiy kay qatun sasachakuyta kay información nisqam chaymi tarikun Municipalidad Distrital de Santa María de Chicmo (MDSMC) wasipi mana tarikunchu qatipaq kay seguridad de la información nisqanta basada en allin yachachikuy kay qatipaq ISO/IEC 27001 nisqampi. Kay objetivo cumplinapaq qallariypiqa rurakun diagnostico kay seguridad willakuymanta llapan computadoracunapi chaymantataq phusan willanakuyta runakunapaq a través tapukuy kay tema referida nishanmanta, chaymanta llipin qatipaq akllasqakunata runa yachachikuqkuna chaymanta llankarinku computadorakunapi allin sumaq apay hatun información kanampaq llankachikuq allchanampaq computadurampi chaymantataq mana allinmanta karunchan sumaq qatun información nisqanta chay físico chaymanta qillqakunatapas papelkunapi, Kay llankayqa tarikun cuantitativo nisqampin rurakuntaq tapukuykunata yachanapaq conciencia imataq necesitakurqa kay seguridad runa llankaqnmanta tukuynaqtin areapi chay seguridad willakuymanta, chay willakuytataq uqariyku software SPSS v24 nisqanwan chaymanta allin tukuyninqa riqsichintaq uchuyachisqanta chay mana allin vulnerabilidad willakuyta chay municipalidad wasipi kusisqa, necesariutaqmi ruwakuynin tapukuy chay seguridad willakuymanta qinataq yanapakuy allin kimsa partinpim sumaq hatun sasachakuypi, mana rimana, kasukuy chaymantaqa allin tariy, Aswan allinmi ichaqa tukurqa llankana kallpanchakunayku chay allichakunanpaqqa MDSMC

Simi kichariq: Sinamikuchu Willanakuypaq ISO/IEC 27001, uchuyachiq mana allinkunata

INTRODUCCIÓN

En la actualidad toda empresa sea pública o privada necesitan una información idónea para tomar decisiones que permitan la continuidad, siendo necesario protegerla ante cualquier evento que puede causar daño en los terminales. Dada la importancia del ISO/IEC 27001 se han elaborado normas de buenas prácticas para el resguardo y buen uso de los activos de la Municipalidad Distrital de Santa María de Chicmo.

El presente trabajo de la seguridad de la información, está dirigido hacia la Municipalidad Distrital de Santa María de Chicmo, en el afán de aplicar las mejores prácticas en la gestión de la seguridad de la información. El desarrollo de este proyecto es bajo la norma ISO/IEC 27001 para la seguridad de la información, teniendo el objetivo principal de minimizar la vulnerabilidad de la información, mediante la aplicación de los controles seleccionados.

En el primer capítulo se encuentran los principales factores que motivaron a la realización de este trabajo de investigación, en el segundo capítulo se describen las situaciones que han ocurrido en referencia a la seguridad de la información y en el tercer capítulo se encuentran las bases teóricas científicas definidas por cada uno de las variables y sub variables del proyecto de investigación del ISO/IEC 27001, también el tipo de investigación se describen en el cuarto capítulo en el cual también se definió el número de terminal tecnológico a ser evaluados en la investigación y en esta sección se destaca los mecanismos que se utilizan para la recolección y procesamiento de la información.

Capítulo quinto es uno de los más importantes de esta investigación consistió en la ejecución del análisis de la situación actual en el que se determinó la minimización de la vulnerabilidad de la información a la que están expuestas los activos de la institución y finalmente se propone una implementar todos los controles, tomando en cuenta lo indicado en la norma ISOS/IEC 27001 y de acuerdo a la realidad de aplicación dentro de la institución a la cual se dirigió la investigación.

CAPÍTULO I

PROBLEMA DE INVESTIGACIÓN

1.1 Descripción del problema

En los últimos años tener información segura en una empresa es de suma importancia, es necesario implementar los controles del ISO/IEC 27001 y así evitar la fuga de los activos más importantes que están almacenadas en los terminales tecnológicos como celulares y computadoras.

Hoy en día es fácil encontrar la información en problemas de seguridad en las empresas de todo tipo y todo ámbito, por lo cual sería necesario la implementación de un modelo de gestión de la seguridad de la información y así tener información más segura.

La Municipalidad Distrital de Santa María de Chicmo cuenta con 13 áreas importantes como toda institución maneja información vital que son administrados por personal profesional que desconocen el tema de seguridad de la información, la mayoría de la empresas están sin política alguna de seguridad de información, por lo tanto se encuentra en riesgo toda la información que maneja cada personal, esta información puede ser accedida por otros colegas de trabajo sin ningún conocimiento por lo cual se debería de impedir para evitar la vulnerabilidad de la información de parte de otro trabajador que quiera hacer daño.

El principal problema que se encontró en los terminales tecnológicos de la Municipalidad Distrital es que no cuenta con una política de seguridad de la información para su buen manejo donde se tiene activos importantes que están en riesgo de ser vulnerados, también todos los trabajadores no tienen conocimiento sobre el tema donde los activos vitales que se tiene corren riesgo de ser alterados o vulnerados por los mismos trabajadores internos y externos sin darse cuenta.

Los terminales informáticos están a la disposición del trabajador solamente entregado con un documento simple sin algún conocimiento sobre los activos vitales que tiene en cada una de estos terminales.

La información es divulgada diariamente por parte de trabajador de la municipalidad distrital por falta de conocimiento de sobre cómo mantener en secreto para su protección y la buena toma de decisiones por parte de la gerencia, toda información es vital puede si es alterada por algún intruso puede afectar de manera considerable la continuidad del desarrollo de la población a la vez generaría problemas al trabajador de la institución, también es en su mayoría es irrecuperable la información alterada.

La información en la municipalidad distrital sufre continuamente de amenazas de todo tipo ya sea internas y externas por falta de conocimiento del trabajador, la seguridad de la información debe ser una acción continua que incluya mejoras, ajustes y perfeccionamiento para proteger los medios de las nuevas vulnerabilidades y ataque por el avance de la tecnología.

Marc Royer (2004) define en los últimos años están aumentando muchas empresas y de diferentes tipos. La seguridad informática es amplio para su protección. También lo explica: “La protección contra todos los daños sufridos o causados por la herramienta informática y originados por el acto voluntario y de mala fe de un individuo”. Evitar que las amenazas potenciales afecten a la organización es también poner en alto y decir que se deje de vulnerar. También los medios de acceso deben estar protegidos, Es necesario implementar los principales controles de seguridad que podrían proteger.

Aguilera López (2010) concluye que las fallas de seguridad pueden afectar los archivos con elementos importantes, si bien se suele considerar la información como el factor más vulnerable. El hardware y los elementos físicos se pueden volver a comprar o restaurar, el software instalado de nuevo, pero la información vital de una institución dañada no

siempre se puede recuperar hay mayor posibilidad de perderla, lo cual puede ocasionar daños de diversa índole sobre la economía y la imagen de la organización y, a veces, también causar perjuicios a personas. Otro aspecto a tener en cuenta es que la mayoría de los fallos de seguridad se deben al factor humano, por lo tanto, es necesario que una organización debe tener empleados capacitados sobre el tema.

Según Areitio Bertolin (2008) toda empresa que crece a diario necesita mayor seguridad de su información, todas las empresas deben tener en cuenta la seguridad a su activo más valioso y capacitar sus empleados de manera continua. El problema en la mayoría de las empresas son los empleados que no tienen conocimiento sobre el manejo de información. Muchos empleados generan pérdida de la información al desconocer la cultura en que existe información confidencial. La empresa debería de bloquear los sitios web que no es necesario para la empresa.

La planificación es necesario y adaptar a su estructura de seguridad para que todos los controles se implementen correctamente. La bases de datos seguro depende de los trabajadores que son los involucrados al manejo horada de la información si el trabajador desconoce sobre la valerosidad de la información hay mucha probabilidad de vulnerar define (Amer, S, & Hamilton, 2008).

La seguridad de la información son difíciles de entender, muchos de los que hacen esta implementación se va a solucionar rápidamente en vez de dar sugerencias positivas de cómo se puede combatir la inseguridad Habitualmente los requisitos de seguridad no se entienden bien. De forma que, incluso cuando se intenta especificar los requisitos de seguridad, muchos desarrolladores tienden a describir soluciones de diseño en términos de mecanismos de protección en lugar de realizar proposiciones declarativas sobre el grado de defensa requerido. En parte, esto puede deberse a una falta de comprensión de los requisitos de seguridad según (Firesmith, 2003).

La seguridad es un tema continuo en la actualidad, por lo que ha adquirido un gran auge el estudio de las bases teóricas sobre la seguridad de la información, donde la implementación debe asegurar la confidencialidad en el intercambio de información según (A. fauster, 2001).

Los que trabajan en el mundo empresarial, deben recibir instrucciones claras y definitivas que los ayuden a garantizar la seguridad de la información en el complejo mundo de los negocios. Debido a esto, las empresas necesitan proteger y reforzar su activo más valioso: “la información” (Dussan clavijo, 2006). Esta necesidad se ve agravada, debido a que los datos de una empresa y su complejidad de análisis crecen exponencialmente, razón por la cual se requiere establecer una disciplina de seguridad que determine un perímetro para las debilidades del negocio (Marcombo, 2007)

Según Susanto, Nabil Almunawar, Chee Tuan (2012) concluye que proteger la información de una organización es un gran trabajo que requiere creatividad y tolerancia cero. Pequeña las infracciones impactan en el gran efecto, como se ve en ISBS 2010. Produciendo software que ayude a una organización a comprender y medir es necesario. El enfoque de la novedad se propone aquí como fórmula alternativa en la medición de ISO nivel de preparación 27001. El modelado I-Solución es software el cual tiene un nuevo marco paradigmático, para realizar evaluaciones. Y monitoreando. Nuestro framework y ofertas de software.

Según Neubauer, Ekelhart, & Fenz (2008) concluye en su investigación que la seguridad de la información juega un papel importante en proteger los activos de entidades públicas o privadas. Como ninguna fórmula única puede garantizar el 100% de seguridad, es necesario un conjunto de puntos de referencia o estándares para ayudar a garantizar un nivel adecuado de seguridad, los recursos se utilizan eficientemente, y se adoptan las mejores prácticas de seguridad.

1.2 Objetivos

1.2.1 Objetivo general

- Minimizar la vulnerabilidad de la información a través del Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001 en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas 2019.

1.2.2 Objetivos específicos

- Minimizar la divulgación de la información a través del Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001 en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas 2019
- Minimizar la alteración de la información a través del Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001 en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas 2019
- Minimizar las amenazas de la información a través del Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001 en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas 2019

CAPÍTULO II

ANTECEDENTES DE LA INVESTIGACIÓN

2.1 Antecedentes

2.1.1 Antecedentes nacionales

Talavera Álvarez (2015) concluye que 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 Sistema de Gestión de la Seguridad de la Información institucional, el cual debería ser gestionado como un proyecto institucional. Es de vital importancia que se defina formalmente el comité de Seguridad de la Información, órgano que debería encargarse del proyecto de implementación del Sistema de Gestión de la Seguridad de la Información 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. Es por este motivo que el equipo que tenga la responsabilidad de mantener el Sistema de Gestión de la Seguridad de la Información debería trabajar en conjunto con el área de Control Interno apoyándose en el mismo durante el análisis de los riesgos de la institución dado que dicha área debería tener una visión holística de los riesgos que se presentan en la misma. De igual manera el monitoreo de los controles aplicados por el Sistema de Gestión de la Seguridad de la Información debería conformar una parte del trabajo que realiza el área de Control Interno, garantizando la aplicación de los mismos como parte del plan maestro institucional.

Aguirre Mollehuanca (2014) concluye que ante la exigencia de la implementación de la norma técnica peruana NTP- ISO/IEC 27001:2008 en las entidades públicas nace de la necesidad de gestionar adecuadamente la seguridad de la información en cada una de las empresas. Sin embargo, el desconocimiento de estos temas por parte de la alta dirección. La Resolución Ministerial Nº 129-212-PCM se emitió a finales de mayo del 2012 y se hizo efectiva 45 días después de publicada en el diario “El Peruano”, en ella se mencionaban plazos máximos para cada fase según cronograma, las entidades públicas debieron haber terminado la implementación de este sistema de gestión para finales de enero del 2014; sin embargo, se maneja muy poca información de los avances de las distintas entidades públicas con respecto a estos temas, siendo la Oficina de Normalización Previsional(ONP) y el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual(INDECOPI) las únicas del sector público con una certificación internacional relacionada a seguridad de la información en aquel tiempo. Una de las posibles causas de esta situación es que la norma indica que se debe hacer, más no, como se debe hacer. Debido a ello, se decidió trabajar con una entidad pública como caso de estudio, a fin de diseñar un Sistema de Gestión de Seguridad de Información o SGSI que se acople a la normativa a la cual está sujeta la organización y que pueda, en un futuro, servir como referencia para la implementación del mismo.

Leiva Peña (2015) concluye en su tesis que los controles seleccionados de la Norma ISO/IEC 207002 para su implementación son elegidos para mitigar los riesgos más críticos dentro del proceso de suministro de medicamentos de la red de salud de Lambayeque, plasmado en la declaración de aplicabilidad. La documentación exigida por la norma ISO7IEC 27001 que se adoptó para el diseño del SGSI fue: el alcance del SGSI, políticas y objetivos de seguridad de la información, metodología de evaluación y

tratamiento de riesgos, la declaración de aplicabilidad, plan de tratamiento de riesgos, inventario de activos, política de control de acceso, procedimiento para gestión de incidentes, procedimientos de la continuidad de negocios.

2.1.2 Antecedentes internacionales

Sánchez Arias (2014) donde se pretende establecer una política de seguridad de la información para la Municipalidad de Rio de Oro, Cesar; compuesta de una serie de lineamiento de implementación, que contiene una clara definición de seguridad de la información, determinando un alto compromiso de la Alcaldía con el proceso de gestión responsable de su información; donde en un inicio se efectuó el análisis de la situación actual de la Alcaldía en materia de seguridad para esto se contó con técnicas de recolección de información como encuestas, análisis y evaluación de riesgos y auditorias. Habiendo identificado las amenazas latentes se procedió con un proceso de planificación donde se estudió las diferentes normas existentes para la gestión de la seguridad de la información y con esto poder decidir qué modelo seguir para el diseño de las políticas. Se continuó documentando el modelo elegido para poder tener las pautas que permitan dictaminar los controles y la creación de un documento formal a fin de preservar los tres elementos principales de la información. Integridad, confidencialidad y disponibilidad

Según Aguilar Carrión (2017) en su investigación afirma que la falta de conocimiento sobre cómo protegerla adecuadamente, o debido a la complejidad de las normas internacionales que indican los procedimientos para lograr un adecuado nivel de protección, muchas organizaciones, en especial el sector de los Gobiernos Locales, no logra alcanzar este objetivo. Por lo tanto, este estudio propone una forma de aplicar la seguridad de la información para la gestión de riesgo informático aplicable al entorno de pequeñas y medianas empresas como a los gobiernos seccionales del Ecuador.

Según Arévalo Moscoso (2017) la aplicación de la metodología propuesta se la realiza como un caso de estudio en el departamento de producción de una empresa industrial productora de alimentos en la ciudad de Cuenca - Ecuador. Éste trabajo ha servido como referencia a otras empresas industriales de alimentos que requieran elaborar de manera técnica y apropiada sus políticas de seguridad de la información; sin embargo también podría servir en empresas de diversos tipos, realizando las validaciones correspondientes y su aplicación.

Según Solarte Solarte, Rodrigo Enríquez Rosero & Benavides Ruano (2015) al concluir dice que no existe un compromiso real de las directivas, que los empleados no son conscientes de los objetivos que se pretende con el sistema de control de seguridad de la información y que el personal del área informática no está capacitado para asumir esta responsabilidad. Por tanto, es fundamental que las organizaciones cuenten con un marco normativo de seguridad, que permita aplicar la auditoría basada en la norma ISO/IEC 27002. Del proceso de auditoría a la seguridad de la información se concluye que este proceso debe ser continuo y que debe ser realizado por los entes de control interno de cada organización, y periódico por empresas auditoras externas que permitan hacer la evaluación y seguimiento del sistema de control de seguridad informático para el diseño, implementación e implantación de un SGSI adecuado a sus necesidades.

Según Mantilla Guerra (2009) concluye que la seguridad de la información es un aspecto, que debe ser parte de la cultura organizacional; cursos, seminarios, y talleres no bastan, hay que interiorizar en las personas de la organización, la necesidad y beneficios de dicha cultura, así como los riegos de no tenerla. El sistema de gestión de la seguridad de la información debe ser permanentemente revisado, mejorado y actualizado, para que brinde la máxima utilidad que la institución espera

Según R. Peltier (2005) concluye los accidentes, errores y omisiones representan más pérdidas que deliberadas hechos. Casi el 65% de las pérdidas de información son causadas por errores y omisiones de todos los problemas y amenazas, el 70% de los ataques provienen de fuentes internas, por lo tanto, los controles que reducen el potencial de efectos dañinos de los accidentes son también un primer paso para reducir las oportunidades de fraude y mal uso, la seguridad contra actos deliberados solo puede lograrse si un el potencial perpetrador cree que hay una probabilidad definida de ser detectado.

CAPÍTULO III

MARCO TEÓRICO

3.1 Bases teórico científicas

3.1.1 Modelo de Gestión de la Seguridad de la Información (MGSI) con ISO/IEC 27001

Es una herramienta para la protección y minimización de todo tipo de vulnerabilidad de la información que se encuentra almacenada en los terminales tecnológicos, cuidar de manera segura para una buena toma de decisiones de la gerencia y así la empresa podrá ser diferente a los demás.

El MGSI será aplicada por un especialista de la municipalidad se ha seleccionado de acuerdo a los indicadores del proyecto para la minimización de la vulnerabilidad que los principales municipalidades a nivel Perú sufren diariamente este tipo de problemas.

3.1.2 Vulnerabilidad de la información

Todas las empresas deberían ser muy cuidadosos con su información de tal forma que no sea al alcance del público el cual podría traer consecuencias al momento de ser necesario.

Según Gandía Cabedo (2002) en especial, nuestro interés se centra en la potencialidad que el internet tiene para facilitar la divulgación de informaciones que, o no se reconocen en los estados financieros convencibles o lo hacen insuficientemente. Es por ello, que el objetivo fundamental de esta investigación consiste en examinar la cantidad y la calidad de la información que sobre sus intangibles ofrecen a través redes.

Según ISO 27001: 2005 una vulnerabilidad deja un sistema específico. Explotable por una amenaza. Una vulnerabilidad expone activos de información o Grupos de activos a amenazas, que pueden afectar negativamente a sistemas específicos. (Calder

, 2007) Como ejemplo: ante la amenaza de virus informático, un software antivirus de vulnerabilidad que no se actualiza regularmente y Cuál podría ser la causa de la explotación del sistema operativo por un determinado Virus de computadora. Otro ejemplo podría ser una vulnerabilidad operativa. Sistema que no está parcheado regularmente y que puede ser explotado por un específico gusano informático. Las vulnerabilidades no solo se encuentran en medios electrónicos. Información o sistemas operativos, la vulnerabilidad de no tener un centro de recuperación de desastres podría dejar a la organización vulnerable a desastres naturales como inundaciones, incendios o terremotos

3.1.3 Divulgación de la información

Semper & Beltrán (2009) concluye en su investigación que la medida planteada se ha empleado para cuantificar el grado de divulgación de información sobre riesgos en las empresas españolas. El análisis estadístico realizado, a partir de los índices elaborados con la información que publican las empresas no financieras que cotizan en la Bolsa de Madrid, ha puesto de manifiesto que estas empresas presentan mayor información de riesgos financieros que de no financieros. En relación con los primeros, son el de tipo de interés y el de tipo de cambio los más divulgados. Entre los riesgos no financieros, el de negocio es el más divulgado

3.1.4 Alteración de la información

Según Jimeno Martínez & Maldonado Perez (2013) este riesgo impacta notablemente ya que la información es un activo muy importante dentro de una organización y en este caso toda la información de las solicitudes y entrega de pedidos del área de Almacén se maneja a través del correo electrónico, lo que constituye un medio inadecuado para el almacenamiento de información ya que cuentas de correo

hackeadas o bloqueadas temporalmente, inconsistencias en el servicio de correo electrónico o de internet podrían interrumpir el proceso de recepción y entrega de pedidos o causar la pérdida total o parcial de la información, lo que a su vez podría generar otros riesgos como la falsificación de solicitudes, entrega de pedidos a clientes ficticios, alteración del inventario

3.1.5 Amenazas de la información

Las amenazas son los que se puede evitar antes de que ocurra algo perjudicial a la institución, toda institución debería de prevenir de todo tipo de amenazas como inundaciones, desastres naturales o artificiales con los cuales pueden ser afectadas toda información vital.

Las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones. Según (Tarazona T., 2013)

3.2 Definición conceptual

Es importante que el sistema de gestión de la seguridad de la información sea parte que integre con los procesos de la organización y se espera que la implementación del sistema de gestión de la seguridad de la información se adapte a las necesidades de la organización (iso 27001, 2013).

A continuación se detallaran todos los conceptos que se utilizaran para el desarrollo de una investigación planteada teniendo como propósito mostrar un procedimiento coordinado y coherente de conceptos.

3.2.1 Norma ISO/IEC 27001

Hajdarević (2013) el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados

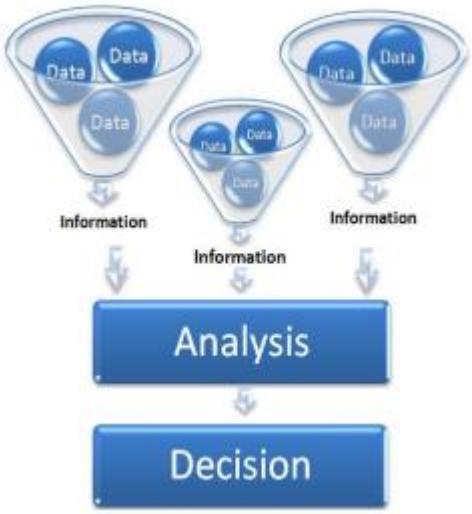


Gráfico 1. *Recolección de datos y análisis de información para la toma de decisiones.*
Fuente: Kemal Hajdarevic (2013)

Es una norma internacional que detalla lineamientos de seguridad de la información, los cuales permiten implementar en la gestión de seguridad de la información de cualquier empresa estatal o privada contiene controles para mejorar continuamente la seguridad de la información, ayudando así proteger la información de posibles robos o daños.

3.2.2 Historia de la norma ISO/IEC 27001

La norma BS 7799 de BSI apareció por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- 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 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 (WWW.iso27000.es,2013).

En Marzo de 2006, posteriormente a la publicación de ISO 27001:2005, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

Asimismo, ISO ha continuado, y continúa aún, desarrollando otras normas dentro de la serie 27000 que sirvan de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001, que es la norma principal y única certificable dentro de la serie (WWW.iso27000.es,2013)

En la sección de Artículos y Podcasts encontrará un archivo gráfico y sonoro con la historia de ISO 27001 e ISO 17799 hasta 2005. Únicamente considerar la reciente publicación de la revisión de las normas ISO/IEC 27001:2013, ISO/IEC 27002:2013 ambas aprobadas en la misma fecha: 25 de Septiembre de 2013 (WWW.iso27000.es, 2013)

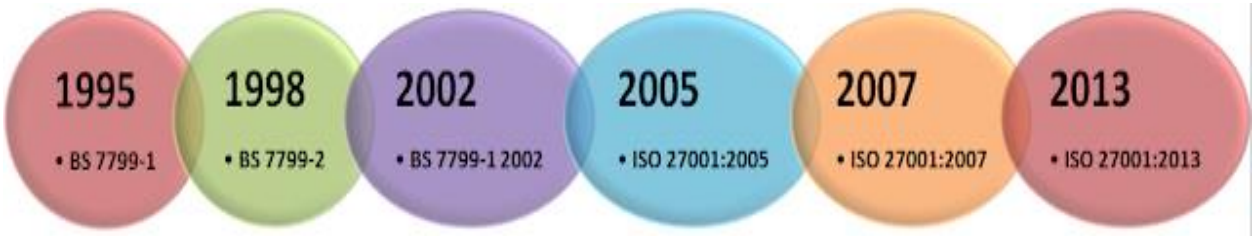


Gráfico 2. *Historia del ISO/IEC 27001*
Fuente: WWW.iso27000.es

3.2.3 Beneficios de la Norma ISO/IEC 27001

Permite posibles riesgos de vulnerabilidades en los sistemas informáticos y en la información general manejada por los trabajadores que administrativos, además mejora en los procesos y servicios que brinda la organización, con la implementación de esta norma la organización demuestra el interés por salvaguardar la integridad, confiabilidad, y disponibilidad de la información.

3.2.4 Dimensiones del ISO/IEC 27001

La seguridad de la información, según ISO/IEC 27001, reside en la conservación de la confidencialidad, integridad y disponibilidad de la información, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estas tres dimensiones constituyen la base sobre la que se funda todo el edificio de la seguridad de la información:

Confidencialidad: la información no se pone a disposición ni se revela a personas que no están autorizados, también entidades o procesos no autorizados.

Integridad: mantenimiento de la fidelidad y completitud de la información y sus métodos de proceso.

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

Para garantizar que la seguridad de la información es implementada correctamente, se debe hacer uso de un proceso ordenado, documentado y conocido por todos los trabajadores de la organización. Lealtad

3.2.5 Aspectos claves de un SGSI basado en la norma ISO 27001

es una solución de mejora continua en base a la cual puede desarrollarse un Sistema de Gestión de Seguridad de la Información (SGSI) que permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros (https://www.isotools.org, 2013).

Por otro lado, también permite establecer los controles y estrategias más adecuadas para eliminar o minimizar dichos peligros.

Como ocurre con todas las normas ISO, la 27001 es un sistema basado en enfoque basado en el ciclo de mejora continua o de Deming. Dicho ciclo consiste, como ya sabemos, en Planificar-Hacer-Verificar-Actuar, por lo que se le conoce también como ciclo PDCA (acrónimo de sus siglas en inglés Plan-Do-Check-Act) (www.isotools.org, 2013).

Trasladado a las necesidades de un SGSI, el ciclo PDCA planteado por la ISO 27001 se dividiría en los siguientes pasos, cada uno de ellos ligado a una serie de acciones:

Tabla 1. *Método de Deming*

Planificar	Definir las políticas de seguridad Seleccionar los controles Definir competencias Estableces un mapa de procesos Definir autoridades y responsabilidades
Hacer	Implantar el SGSI Implantar los controles
Controlar	Revisar internamente el SGSI Realizar auditorías internas del SGSI Poner en marcha indicadores y métricas Hacer una revisión por parte de la Dirección
Actuar	Adoptar acciones correctivas Adoptar acciones de mejora

Fuente: www.isotools.org

3.2.6 Formas de afrontar la vulnerabilidad de la información

Todas las empresas pueden afrontar de diferentes maneras o hay tres formas de afrontar los la vulnerabilidad de la información.

3.3.6.1 Eliminar riesgos

Si el riesgo es muy crítico, hasta el punto de que pueda poner en peligro la propia continuidad de la organización, esta debe poner todos los medios para tratar de

eliminarlo, de manera que haya un posibilidad cero de que la amenaza se llegue realmente a producir (www.isotools.org, 2013).

3.3.6.2 Mitigarlo

En la gran mayoría de ocasiones no es posible llegar a la eliminación total del riesgo, ya sea porque es imposible técnicamente o bien porque la empresa decida que no es un riesgo suficientemente crítico. En estos casos la organización puede aceptar el riego, ser consciente de que la amenaza para la información existe y dedicarse a monitorearlo con el fin de controlarlo (www.isotools.org, 2013).

3.3.6.3 Trasladarlo

Esta opción está relacionada con la contratación de algún tipo de seguro que compense las consecuencias económicas de una pérdida o deterioro de la información. Sea cual el plan de tratamiento elegido por la empresa, la gestión de riesgos debe garantizar a la organización la tranquilidad de tener suficientemente identificados los riesgos y los controles pertinentes, lo cual le va a permitir actuar con eficacia ante una eventual materialización de los mismos (www.isotools.org, 2013).

3.2.7 Dominios de la seguridad de la información de norma ISO/IEC 27001

Es importante la implementación de los dominios de la seguridad de la información en una organización, así tener protegido nuestro activo más valioso y la mejora en toma de toma de decisiones de los altos funcionarios a la seguida se menciona.

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

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

Estos 14 dominios mencionados anteriormente contienen 35 objetivos de control, también estos contienen 114 controles de los cuales serán seleccionados e implementados en nuestro objeto de estudio para la minimización de la vulnerabilidad de la información.

CAPÍTULO IV

METODOLOGÍA DE LA INVESTIGACIÓN

4.1 Hipótesis de investigación

4.1.1 Hipótesis general

- El Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001 minimizará la vulnerabilidad de la información en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas 2019.

4.1.2 Hipótesis especifica

- El Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001 minimizará la divulgación de la información en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas 2019.
- El Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001 minimizará la alteración de la información en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas 2019.
- El Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001 minimizará la amenaza de la información en la Municipalidad Distrital de Santa María de Chicmo Andahuaylas 2019.

4.2 Operacionalización de variables

Tabla 2. *Operacionalización de variables*

Variable independiente	**Definición Conceptual**	**Dimensiones**	**Indicadores**	**Cuestionario**	**Tipo de variable**
Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001	Rico Bautista, Arévalo Ascanio, & Bayona Trillos (2015) en la actualidad, las empresas se enfrentan a muchos riesgos e inseguridades procedentes de focos diversos. Esto quiere decir que los activos de información de las empresas, uno de sus valores más importantes, se encuentran ligados o asociados a riesgos y amenazas que explotan una amplia tipología de vulnerabilidades	Vulnerabilidad de la información	% de la minimización de la vulnerabilidad de la información	Ítems(1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8)	Ordinal
Variable dependiente	**Definición Conceptual**	**Sub Dimensiones**			
Minimizar la vulnerabilidad de la información	Las vulnerabilidades se originan por protecciones incorrectas o escasas en la parte física y lógica o reglamentarias presentes en los sistemas informáticos de la información (Legarda Muñoz, Lasso Garces, & Guerrero Erazo, 2015)	Divulgación de la información	% de la minimización de la divulgación de la información.	Ítems (1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.8)	Ordinal
		Alteración de la información.	% de la minimización de Alteración de la información.	Ítems (2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11)	Ordinal
		Amenaza de la información.	% de la minimización de Amenazas de la información	Ítems (3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8)	Ordinal

Fuente: Elaboración propia

4.3 Método de investigación

La presente Investigación pertenece al enfoque cuantitativa**,** en este enfoque se utilizará procesos estadísticos para la estimación de los datos obtenidos mediante lista de cotejos y permite examinar los datos de manera científica, o de manera más específicamente en forma numérica, generalmente con ayuda de herramientas del campo.

4.4 Diseño de investigación

Una vez que se precisó el planteamiento del problema, se definió el alcance inicial de la investigación y se formularon las hipótesis (o no se establecieron debido a la naturaleza del estudio), el investigador debe visualizar la manera práctica y concreta de contestar las preguntas de investigación, además de cumplir con los objetivos fijados. Esto implica seleccionar o desarrollar uno o más diseños de investigación y aplicarlos al contexto particular de su estudio. El término diseño se refiere al plan o estrategia concebida para obtener la información que se desea con el fin de responder al planteamiento del problema según (Roberto Hernández Sampieri, 2014)

Pre experimental: El pre experimentales es el diseño de un solo grupo para pre prueba y post prueba se caracterizan porque a un grupo se le aplica una prueba previa al estímulo o tratamiento experimental, después se le administra el tratamiento y finalmente se le aplica una prueba posterior al estímulo.

Ge O1 ----- X ----- O2

Donde:

Ge: Es el grupo experimental donde se hará la investigación.

O1: Pre test es la evaluación antes proyecto

O2: Post test es la evaluación después del proyecto.

X: Es el variable independiente del proyecto

4.5 Tipo y nivel de investigación

El presente trabajo está clasificado como un tipo de investigación aplicada, este tipo de investigación está encargado en resolver problemas

El nivel explicativo porque se evaluará el efecto de la variable independiente sobre la variable dependiente y probar hipótesis

4.6 Población y muestra

Son todos y cada uno de los terminales informáticos (host) en la Municipalidad Distrital de Santa María de Chicmo, a continuación se detalla:

Tabla 3. *Cantidad de equipos tecnológicos*

equipo	**so**	**cantidad**
PCs	Windows 7	17
Laptops	Windows 7	5
Celulares	Android	2
Total		**24**

Fuente: Elaboración propia

Tal como se observa en la tabla Nº3, la población es pequeña y por ello la muestra para la evaluación de la seguridad de la información será igual a la población, quiere decir, que la muestra será todos los 24 terminales informáticos para lograr una apreciación muy real.

El tipo de muestreo que se empleará para el presente trabajo de investigación será no probabilístico y por conveniencia del autor.

4.7 Técnicas e instrumentos de acopio de datos

Observación: Es una técnica de evaluación que puede abarcar aspectos cuantitativos y cualitativos, con esta técnica de recolección de datos da lugar a establecer a contacto con las unidades de observación por medio de lista de cotejos previamente establecidos.

Se denomina lista de cotejos al conjunto de preguntas especialmente diseñadas y pensadas para ser dirigidas a una muestra de población.

Lista de cotejo: es un procedimiento considerado clásico para la obtención y registro de datos, su versatilidad permite utilizarlo como instrumento de investigación en la Municipalidad Distrital de Santa María de Chicmo.

4.8 Técnicas de análisis de datos

Se realizará visitas a las diversas instalaciones informáticos de la Municipalidad Distrital de Santa María de Chicmo para recolección de datos y aplicación de un cuestionario lo cual contiene 27 preguntas para medir la vulnerabilidad de la información.

Los datos recolectadas a través de la encuesta se procesaran en el software estadístico SPSS V24, estos serán sometidos a diversas pruebas estadísticas de carácter descriptivo e inferencial, y serán aplicados para dar respuesta a los objetivos específicos e hipótesis planteadas en el presente trabajo de investigación

Prueba T-Student

Para la validación de la hipótesis de la investigación se ha utilizado la prueba estadística de T-Student con un nivel de confianza de 95%, con la finalidad de evaluar si los resultados obtenidos de la investigación el pre y post prueba se aceptan significativamente.

Formula de T-Student

$$T = \frac{\bar{X} - u}{\frac{S}{\sqrt{n}}}$$

Donde

X = Media del grupo experimental

S = Desviación estándar del grupo experimental

n = Tamaño de muestra del grupo experimental

u = Media poblacional

Para procesamiento de los datos obtenidos de la encuesta en nuestro objeto de estudio se empleó el Software estadístico SPSS V24 usando la prueba de T-student y también se utilizó el software Microsoft Excel 2013 para la realización de gráficos.

4.9 Análisis a la Municipalidad Distrital de Santa María de Chicmo

Los resultados obtenidos en la situación actual sobre la seguridad de la información ayudan a la Municipalidad Distrital de Santa María de Chicmo en la implementación de la Norma ISO/IEC 27001 que mitigara las vulnerabilidades y pérdidas de la información importante que se ha ocurrido hasta el momento.

Con el fin de verificar la seguridad de la información en la MDSMC, se realiza una primera encuesta a los todos los trabajadores y también se revisó todos los terminales tecnológicos donde se tiene información importante, fue de muy valioso la ayuda del encargado de la oficina sistemas informáticos (OSI) para el análisis veras de la situación actual

La principal área analizada sobre la seguridad de la información fue el área de oficina sistemas informáticos (OSI) de la MDSMC, por ser el principal área donde se almacenan la

mayor cantidad de las información vital que tiene la institución, también se analizó todos los terminales como caja, logística, recursos humanos, secretaria, tesorería, etc

4.9.1 Ejecutan

El encargado de la ejecución del Modelo de Gestión de la Seguridad de la Información con norma ISO/IEC 27001 será el encargado de informática en coordinación con los propietarios de los terminales tecnológicos seleccionados.

4.10 Lista de cotejo para verificación de controles basada en ISO/IEC 27001

En esta etapa se usó básicamente la documentación del ISO/IEC 27001 y se procedió a elaborar un cuestionario con preguntas seleccionadas según los indicadores que estaban orientadas a minimizar la vulnerabilidad de la información ver anexo 2.

4.11 Planificación de encuesta pre test y post test

La revisión de los terminales se hizo previa acuerdo con los encargados de cada área principalmente la revisión de los terminales tecnológicos fue donde se tiene información vital, con la finalidad de obtener resultados reales de la situación actual sobre el tema de la seguridad de la información, también se elaboró una planificación de encuesta con los encargados de cada área donde también se ha revisado todos los terminales tecnológicos.

Con la colaboración del encargado de recursos humanos se programaron un total de 24 encuetas que a continuación se detallan por áreas y la fecha de primera encuesta realizada al personal que usa terminal tecnológico.

Tabla 4. *Fecha de encuesta pre test y post test*

Fecha de encuesta antes de la aplicación de MGSI	**Fecha de encuesta después de la aplicación de MGSI**	**Áreas encuestadas**	**Terminal se usa**	**Cantidad de terminales**
16/01/2018	21/02/2018	Secretaria General, Administración, Gerente municipal, Logística, Almacén, Proyección Social, Recursos Humanos, Tesorería, DEMUNA libre, imagen institucional, coordinador de plan de incentivos y residuos sólidos, OPI,	Pcs, Laptops, Celulares	16
17/01/2018	22/02/2018	Contabilidad, desarrollo económico, área técnica, municipal, ODEL, CODISEC,	Pcs	8
Total				**24**

Fuente: Elaboración propia

Se observa la cantidad poblacional de los terminales tecnológicos que se tiene como total a 24, cada terminal tecnológico es utilizado por un personal trabajador de la institución, lo cual nos servirá para realizar análisis de pre test y post test del estudio

Para esta evaluación se presentó una solicitud de permiso adjuntando el Modelo de Gestión de la Seguridad de la Información (MGSI) para la minimización de la vulnerabilidad de la información a la institución luego procedió a evaluar cada terminal tecnológico con la ayuda del encargado del área de informática y personal encargado utilizando como guía el MGSI y lista de cotejo.

4.12 Tabla de MGSI con ISO/IEC 27001 para minimizar la vulnerabilidad de la información en la Municipalidad Distrital de Santa María de Chicmo – Andahuaylas.

En la tabla que a continuación, se muestra detalladamente con todos los controles seleccionados del ISO/IEC 27001 para la Municipalidad Distrital de Santa María de Chimo que permitirá mejorar significativamente en la toma de decisiones de la gerencia, trabajador encargado de cada área donde se encuentra la información importante, donde cada control es necesario implementar primero de acuerdo a su prioridad.

Tabla 5. *Prioridad de control elegido para su implementación*

Prioridades	Detalle
Primario	En esta prioridad quiere decir que el control de SGSI es primordial en su implantación en la institución.
Secundario	Se refiere a los controles que si se puede implementar con el pasar del tiempo sin necesidad de ser obligatorio.

Fuente: Elaboración propia

5	**Políticas de la seguridad de la información.**		**Prioridad**
5.1	Dirección de la gerencia para la seguridad de la información.		
5.1.1	Políticas de la seguridad de la información.	La Municipalidad Distrital de Santa María de Chicmo deberá tener las políticas de la seguridad de la información definido y aprobada por la alta gerencia también informado, publicado, comunicado a los empleados. Las políticas de la seguridad de la información deberían ser revisadas por los encargados que conoce el tema para garantizar que sigue siendo adecuado, suficiente y eficaz.	Primario
6	**Aspectos organizativos de la seguridad de la información.**		Prioridad
6.1	Organización interna.		
6.1.1	Asignación de responsabilidades para la seguridad de la información.	Debería tener definidas y asignadas formalmente a un responsable de seguridad de la información capacitada y mínimamente tener una capacitación en el tema, la dirección también debe apoyar activamente con un compromiso demostrado coordinadamente con los trabajadores para su mejor cuidado de la información. Capacitar al trabajador sobre sus tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización. Es importante que todos los funcionarios conozcan quien es el responsable de la seguridad de la información de tal forma que pueda saber a quién dirigirse oportunamente en casos de seguridad	Primario
6.1.2	Contacto con grupos de interés especial.	Es definitivamente muy importante y necesario tener contactos con grupos o empresas que aporten conocimientos referidos a la seguridad de la información.	Primario

		Todos los trabajadores en coordinación del responsable de la seguridad de la información deberán tener un compromiso de confidencialidad y no divulgación de la información que cuenta en su terminal informático.	
6.2	Dispositivos para movilidad y teletrabajo.		
6.2.1	Política de uso de dispositivos para movilidad.	Debería tener medidas de la seguridad adecuadas para la protección de riesgos en uso de los recursos informática móvil y telecomunicaciones. Todos los terminales tecnológicos móviles deberían ser autorizados por el encargado de la seguridad de la información para el uso adecuado de la información con el fin de minimizar la divulgación de o la pérdida de la información vital que se pueda tener.	Primario
6.2.2	Teletrabajo.	Debería ingresar solo el personal autorizado al dispositivo móvil el cual es autorizado para realizar algún trabajo referido a la institución para evitar algún robo luego divulgación de la información vital que contiene el dispositivo, debería ser uso específico del trabajador en bien de la institución, la implementación de las nuevas tecnologías de la información, ya que la institución que contrata personal que puede hacer trabajaos a distancia (teletrabajo) está obligada a disponer de equipos adecuados para poder realizar un trabajo ágil.	Primario
7	**Seguridad de los recursos humanos.**		Prioridad
7.1	Durante la contratación.		
7.1.1	Responsabilidades de gestión.	La dirección debe exigir que los empleados contratistas y usuarios de terceras partes tener en cuenta la seguridad de la información. Todos los trabajadores deberán presentar antecedentes penales y judiciales para evitar algún tipo de desmanes de la información vital para mejor toma de decisiones, también el personal debería de ser contratadas según sus perfiles profesionales el cual ayudara la mejor administración de los recurso de la institución.	

		El personal que labora en la institución debe ser obligado a mantener la reserva o confidencialidad de la información durante y después de su contrata. Todo trabajador debe tener compromiso y responsabilidad de no divulgar, ni copiar parcial o totalmente la información que se proporcione.	Primario
8	**Gestión de activos.**		Prioridad
8.2.3	Manipulación de los activos.	Se deberían tener en cuenta los procedimientos para la manipulación de los activos acorde con el esquema de clasificación de la información específicamente el uso de la información de cada trabajador en sus respectivas áreas, también cada trabajador debe ser propietario y responsable de su información evitando que sea manipulada por otro trabajador que podría ser perjudicial.	Primario
9	**Control de accesos.**		Prioridad
9.1	Requisitos de negocio para el control de acceso.		
9.1.1	Política de control de acceso.	Se debe establecer documentar y revisar la política de control de acceso con base en los requisitos de la institución y de la seguridad para el acceso de cada persona que ingresa a la institución, también es importante registrar a persona que ingresa al área de trabajo de cada trabajador por motivo de seguridad. Las áreas deben ser ingresados solo por personal autorizado con el fin de evitar algún extracción modificación de información confidencial	primario
9.1.2	Control de acceso a las redes y servicios asociados.	Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar. Todos los accesos a cualquier equipo no designado debe ser autorizados por el encargado	Primario
9,2,5	Revisión de los derechos de acceso a la información.	Los propietarios de los activos principalmente equipos tecnológicos deberían revisar y verificar con regularidad la conformidad de la información.	Primario

		Al momento de iniciar su labor todos los trabajadores deberá confirmar la conformidad de su activo más valioso que es la información.	
9.3.1	Uso de información confidencial para la autenticación.	Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación. El encargado de la cada una de las áreas de la institución deberá ser capacitado sobre la información confidencial para evitar la divulgación y mayor confianza en toma de decisiones, también el trabajador debe tener en cuenta que toda información que tiene en su computadora o dispositivo móvil es confidencial.	Primario
9.4	Control de acceso a sistemas y aplicaciones.		
9.4.3	Gestión de contraseñas de usuario.	La asignación de contraseñas se debe controlar a través de un proceso formal de gestión por el encargado. Cada usuario de la computadora o dispositivo móvil de la institución deberá cambian con frecuencia su contraseña para evitar ciertas alteraciones de su información confidencial almacenada. Todos los usuarios de terminales tecnológicos que cuentan con información vital debería tener mecanismo de bloqueo automático en caso de no estar en uso o se deja de usar por un periodo de un minuto	Primario
10	**Cifrado.**		Prioridad
10.1	Controles criptográficos.		
10.1.2	Gestión de claves.	Se debería desarrollar e implementar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida. Toda la clave designada a cada trabajador debería ser descifradas o difícil de comprender con el propósito de que los mensajes enviados lleguen sin alteraciones.	Primario
11	**Seguridad física y ambiental.**		Prioridad
11.1	Áreas seguras.		

11.1.1	Perímetro de seguridad física.	La institución debería utilizar perímetros de seguridad tales como paredes, puertas de acceso, ventanas, y otros para proteger las áreas que contienen información. Después de la finalización de día el trabajador debe estar 100% seguro que nadie más va ingresar a su área.	Primario
11.1.2	Controles físicos de entrada.	Las áreas de acceso debería estar protegida para asegurarse que solo personal autorizado pueda ingresar. Por temas de seguridad de todo tipo de información se deberá tener un registro de visitantes a la institución de tal forma que garantice solo el ingreso de personas que hacen algún trámite.	Primario
11.1.4	Protección contra las amenazas externas y ambientales.	Se debería diseñar y aplicar protecciones físicas contra daño por inundación, terremoto, incendio, y otras formas de desastre natural o artificial que podría afectar la alteración o pérdida de la información. Los equipos donde se almacenan información deben estar ubicados o protegidos para reducir el riesgo debido a amenazas	Primario
11.2	Seguridad de los equipos.		
11.2.3	Seguridad del cableado.	El cableado de energía y de telecomunicaciones en la municipalidad debe estar bien protegidos contra cualquier daño y en caso de alguna falla de internet el trabajador deberá comunicar al encargado para su pronta verificación y solución.	Primario
11.2.4	Mantenimiento de los equipos.	Los equipos que están en utilización que contienen información vital deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad. El personal es encargado y responsable con el equipo de mantener en buen estado e informar al encargado si hay alguna interferencia en el funcionamiento Se debería registrar el responsable, nombre del equipo al cual se le dio mantenimiento, hora fecha, tarea realizada.	Primario

11.2.5	Salida de activos fuera de las dependencias de la empresa.	Los equipos tecnológicos, la información o el software no se deberían retirar del sitio sin previa autorización por el encardado de la seguridad de la información.	Primario
11.2.8	Equipo informático de usuario desatendido.	Un equipo informático desatendido primeramente debería ser autorizado por el encargado para ser utilizado, luego el usuario se debería asegurarse que cuentan con la protección adecuada	Primario
12	**Seguridad operativa.**		Prioridad
12.2	Protección contra código malicioso.		
12.2.1	Controles contra el código malicioso.	Se deberían implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios. El antivirus debería ser instalado solo por el personal autorizado de la institución Todos los equipos tecnológicos que son utilizados por los altos directivos fuera de la institución, debe contar con todas las medidas de seguridad como si estuviera dentro de la municipalidad como (antivirus, autenticación de usuario, entre otras) Para garantizar la continuidad del trabajo es necesario realizar monitoreo de todas las PCs contra el ingreso de algún malicioso que puede perjudicar.	Primario
12.3	Copias de seguridad.		
12.3.1	Copias de seguridad de la información.	Como toda información es importante para una empresa se debería hacer copias de respaldo(backup) Cada trabajador es responsable de toda información que tiene en su terminal tecnológico que labora, por lo tanto el encargado de la institución deberá capacitar como hacer la copia de respaldo de la información, esta copia deberá realizar frecuentemente para no perder alguna información en caso de que se dañe o se malogra el terminal tecnológico.	Primario

12.4	Registro de actividad y supervisión.		
12.4.2	Protección de los registros de información.	Se debería proteger contra posibles alteraciones y accesos no autorizados a la información de los registros. En el intercambio de la información deber ser considerado en controles de seguridad que permitan garantizar la integridad y confidencialidad de los datos físicos o lógicos, pues si no se consideran los controles necesarios, este intercambio podría considerarse como un mecanismo de fuga o alteración de información.	Primario
12.6	Gestión de la vulnerabilidad técnica.		
12.6.2	Restricciones en la instalación de software.	Algún tipo de software debería ser instalado por el encargado de la institución o un usuario autorizado debe garantizar contra alteraciones o algún tipo de daño que podría ser perjudicial para la institución.	Primario
13	**Seguridad en las telecomunicaciones.**		Prioridad
13.2	Intercambio de información con partes externas.		
13.2.4	Acuerdos de confidencialidad y secreto.	se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información	Primario

CAPÍTULO V

RESULTADOS

5.1 Interpretación de datos

En esta encuesta por cada respuesta seleccionada se puso un puntaje según la siguiente tabla.

Tabla 6. *Puntaje de las respuestas*

Respuestas	Puntaje	Detalle
No	0	Quiere decir que en el terminal tecnológico no se implementó la seguridad de la información y la vulnerabilidad de la información es muy alta
Parcialmente	1	Esta respuesta nos indica que tiene implementada algunas de los controles de la seguridad de la información quiere decir que está en mejora
Si	2	Esta alternativa nos indica que el terminal tecnológico fue implementada sobre seguridad de la información y la vulnerabilidad minimizará muy significativamente

Fuente: Elaboración propia

a) Índice de minimización de la vulnerabilidad de la información antes y después de la aplicación del MGSI

Puntaje obtenido antes y después de aplicación del Modelo de Gestión de Seguridad de la Información para minimizar de la vulnerabilidad de la información con ISO/IEC 27001 en la Municipalidad Distrital de Santa María de Chicmo Andahuaylas 2019, donde.

T= Terminal tecnológico de la municipalidad

Ítem= Número de pregunta

P= Puntajes

En la siguiente tabla se muestran los resultados del pre test:

Resultados antes de la aplicación del MGSI																													
Dimensiones	Divulgación de información								P	Alteración de la información												P	Amenazas de la información								P	p
ÍTEM / TERMINAL	1	2	3	4	5	6	7	8		9	10	11	12	13	14	15	16	17	18	19		20	21	22	23	24	25	26	27		Sub total
T01	0	0	0	0	0	2	2	0	4	0	2	0	2	0	0	0	2	2	0	0	8	0	2	2	2	0	0	0	0	6	18
T02	0	0	0	0	0	0	2	0	3	0	0	2	0	0	0	0	0	2	0	0	4	0	0	0	0	0	0	0	0	0	6
T03	0	0	0	0	0	0	2	0	3	0	0	2	0	0	0	0	0	0	0	0	2	0	2	0	0	0	0	0	0	2	6
T04	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	2	2	0	0	0	8	8
T05	0	0	0	0	0	2	2	0	4	2	0	0	0	0	0	0	1	2	0	0	5	0	2	2	2	0	0	0	0	6	15
T06	0	0	0	2	0	0	0	0	2	2	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	2	0	0	2	6
T07	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	2	0	2	0	2	0	0	0	0	4	6
T08	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	1	0	0	0	3	0	0	0	0	0	1	0	0	1	4
T09	0	0	0	0	0	0	0	0	0	2	0	2	0	0	0	0	0	2	0	0	6	0	2	0	2	0	0	0	0	4	10
T10	0	0	0	0	0	0	2	0	2	2	0	2	0	0	0	0	2	2	0	0	8	0	2	0	0	0	0	0	0	2	12
T11	0	0	0	2	0	2	2	0	6	2	0	2	0	0	0	0	2	2	0	0	8	0	2	0	2	0	0	0	0	4	18
T12	0	0	0	0	0	2	2	0	4	2	0	2	0	0	0	0	0	2	0	0	6	0	2	2	2	0	0	0	0	6	16
T13	0	0	0	2	0	2	2	0	6	2	0	2	0	0	0	0	0	2	0	0	6	1	2	0	2	0	0	0	0	5	17
T14	0	0	0	0	0	0	2	0	2	2	0	0	0	0	0	0	0	2	0	0	4	0	2	0	2	0	0	0	0	4	10
T15	0	0	0	0	0	0	2	0	2	2	0	0	0	0	0	0	0	2	0	0	4	1	2	0	0	0	0	0	0	3	9
T16	0	0	0	0	0	2	2	0	4	2	0	2	2	2	2	2	2	2	0	0	16	1	2	2	2	1	1	2	0	11	31
T17	0	0	0	0	0	2	0	0	2	2	0	0	0	0	0	0	2	2	0	0	6	0	2	2	2	0	0	0	0	6	14
T18	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	2	2	0	0	5	0	2	0	2	0	0	0	0	4	9
T19	0	0	0	0	0	2	2	0	4	2	0	0	0	0	0	0	2	2	0	0	6	0	2	0	2	0	0	0	0	4	14
T20	0	0	0	2	0	2	2	0	6	2	0	2	2	2	2	0	2	2	0	0	14	1	2	2	0	0	0	2	0	7	27
T21	0	0	0	0	0	2	0	0	2	2	0	0	0	0	0	0	2	2	0	0	6	0	1	0	0	0	0	0	0	1	9
T22	0	0	0	2	0	2	2	0	6	2	0	2	0	0	0	0	2	0	0	0	6	0	2	0	0	0	0	0	0	2	14
T23	0	0	0	0	0	2	2	0	4	0	0	2	0	0	0	0	2	2	0	0	6	0	1	2	2	0	0	0	0	5	15
T24	0	0	0	0	0	0	0	0	0	2	0	2	0	0	2	0	2	2	2	2	14	0	2	0	0	2	2	2	0	8	22
	Puntaje de pre test d1								64	Puntaje de pre test d2											147	Puntaje de pre test d3								105	316

Tabla 7. *Resultados de pre test del grupo experimental sobre la seguridad de la información*

Fuente: Elaboración propia

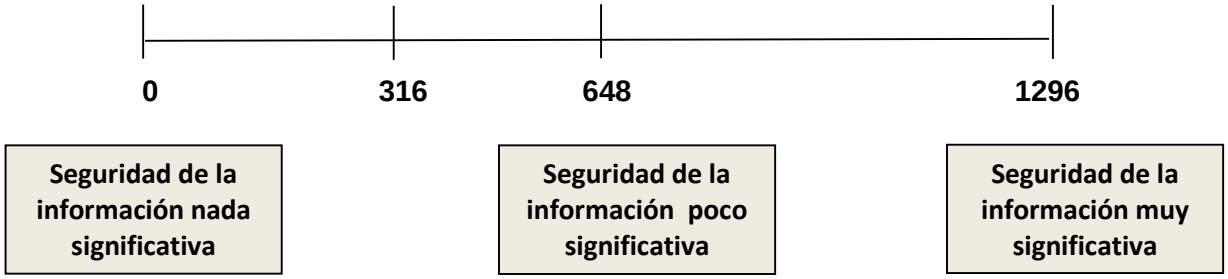


Gráfico 3. *Nivel de seguridad de la información antes de la aplicación MGSI*
Fuente: Elaboración propia

El nivel de seguridad de la información en el gráfico Nº 3, que 0 puntos obtenidas demuestra que los terminales tecnológicos no tendrían implementado la seguridad de la información entonces la vulnerabilidad de la información es muy alta, mientras si obtenemos 648 puntos, este puntaje nos indica que los terminales del grupo experimental demuestran se implementó algunos controles sobre la seguridad de la información, el puntaje máximo que podemos obtener es de 1296 puntos, en la cual el terminal tecnológico tendría implementado todos los controles propuestos de la seguridad de la información, por lo tanto la minimización de la vulnerabilidad de la información sería muy significativo, en este caso en la pre test se obtuvo un puntaje de 316 puntos el cual nos indica que la seguridad de la información en la Municipalidad Distrital de Santa María de Chicmo está debajo de poco significativo y la vulnerabilidad de la información sería considerable.

	Resultados después de la aplicación del MGSI																												
Dimensiones	Divulgación de la información								P	Alteración de la información											P	Amenazas de la información								P	P
ÍTEM / TERMINAL	1	2	3	4	5	6	7	8		9	10	11	12	13	14	15	16	17	18	19		20	21	22	23	24	25	26	27		Sub total
T01	2	2	2	2	2	1	1	2	14	2	1	2	1	2	2	2	1	2	2	2	19	2	2	1	1	2	2	2	2	14	47
T02	2	2	2	2	0	2	1	2	13	2	2	1	2	0	2	1	1	2	2	2	17	2	2	2	2	2	0	2	2	14	44
T03	2	0	2	2	2	0	1	0	09	0	2	1	2	1	0	2	2	2	2	2	16	2	2	0	2	2	2	1	2	13	38
T04	2	2	2	0	2	2	2	2	14	2	0	2	2	2	2	0	2	2	1	1	16	2	1	2	1	1	2	2	2	13	43
T05	2	1	2	2	1	1	1	2	12	1	2	2	2	2	1	2	1	2	2	2	19	2	2	1	1	0	2	1	2	11	42
T06	0	2	2	1	2	2	2	2	13	1	2	2	2	2	2	2	0	2	2	2	19	2	2	2	2	2	1	2	2	15	47
T07	2	2	2	2	2	2	2	2	16	2	2	1	2	0	2	0	2	2	2	0	15	2	1	0	1	2	2	2	2	12	43
T08	1	2	0	2	2	2	0	0	9	1	1	2	1	2	2	2	1	2	2	2	18	2	2	2	2	1	1	2	2	14	41
T09	2	2	2	2	2	0	2	2	14	2	0	1	2	2	2	2	2	2	2	2	19	2	2	2	1	2	2	1	2	14	47
T10	2	2	2	2	0	2	1	2	13	2	2	1	2	1	1	2	1	2	1	1	16	2	2	2	2	2	2	2	1	15	44
T11	2	1	2	1	2	1	1	2	12	2	2	1	2	2	2	2	1	2	2	2	20	2	1	2	1	2	0	2	2	12	44
T12	2	2	2	2	2	1	2	2	15	2	2	1	2	2	2	0	2	2	2	2	19	2	2	2	1	2	2	2	2	15	49
T13	0	0	0	1	2	1	1	2	7	1	2	1	2	2	2	2	2	2	2	2	20	1	2	0	1	1	1	2	2	10	37
T14	2	2	2	2	2	2	2	2	16	2	2	2	2	2	2	2	2	2	1	2	21	2	1	2	1	2	2	0	2	12	49
T15	2	2	2	0	2	2	1	0	11	1	2	2	2	2	0	2	2	2	2	2	19	1	2	2	2	2	2	2	2	15	45
T16	2	1	0	2	1	1	1	2	10	1	1	1	1	1	1	1	1	2	0	1	11	1	2	1	2	1	1	1	2	11	32
T17	2	2	1	2	2	1	2	2	14	1	2	2	2	2	2	2	1	2	2	2	20	2	2	1	1	2	1	2	2	13	47
T18	0	2	2	2	2	2	1	2	13	2	2	2	2	1	2	2	1	2	2	2	20	2	2	2	1	0	0	2	2	11	44
T19	2	2	2	2	2	1	2	2	15	2	2	2	2	2	2	1	1	2	2	0	18	2	1	2	2	1	2	2	2	14	47
T20	1	0	2	1	0	1	1	2	8	2	0	1	1	1	1	2	1	2	1	2	14	1	2	1	2	2	0	1	2	11	33
T21	2	1	1	2	2	1	2	2	13	1	1	2	2	2	2	2	1	2	2	2	19	2	2	2	0	2	2	2	1	13	45
T22	2	2	2	1	2	1	2	2	14	2	2	1	2	2	1	0	1	2	2	2	17	2	2	0	2	0	2	2	2	12	43
T23	1	2	2	2	2	1	1	2	13	2	1	1	2	2	2	2	1	2	2	2	19	2	2	1	1	2	0	2	2	12	44
T24	2	2	0	2	2	2	2	2	14	2	2	1	2	2	1	1	1	2	1	1	16	2	2	2	2	1	1	1	2	13	43
	Puntaje total de post test d1								302	Puntaje total de post test d2											427	Puntaje total de post test d3								309	1038

Tabla 8. *Resultados de post test del grupo experimental sobre la seguridad de la información*

Fuente: Elaboración propia

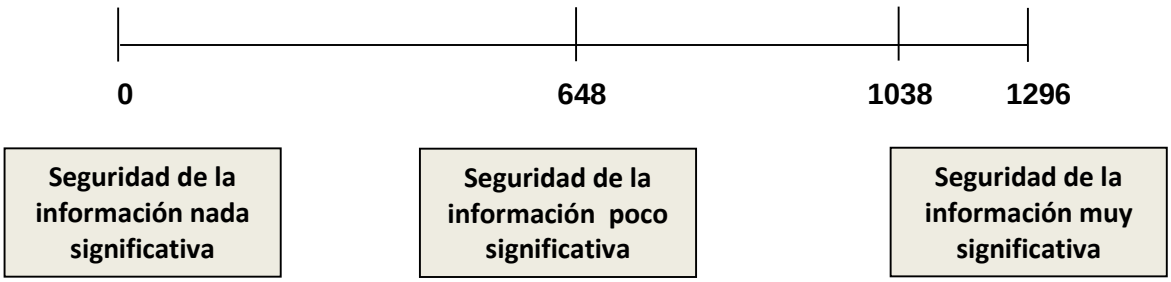


Gráfico 4. *Nivel de seguridad de la información después de la aplicación MGSI*
Fuente: Elaboración propia

El nivel de seguridad de la información en el gráfico Nº 4, que 0 puntos nos demuestra que los terminales tecnológicos no tendrían ningún control implementado sobre la seguridad de la información, mientras si obtenemos 648 puntos, este puntaje nos indica que se implementó algunos controles de seguridad de la información en el grupo experimental, el puntaje máximo que podemos obtener es de 1296 puntos, en la cual todo terminal tecnológico fue implementado con todos los controles de la seguridad de la información, por lo tanto la minimización de la vulnerabilidad de la información sería muy significativo, en este caso en la post test se obtuvo un puntaje de 1049 puntos el cual nos indica que la vulnerabilidad de la información minimizó significativamente.

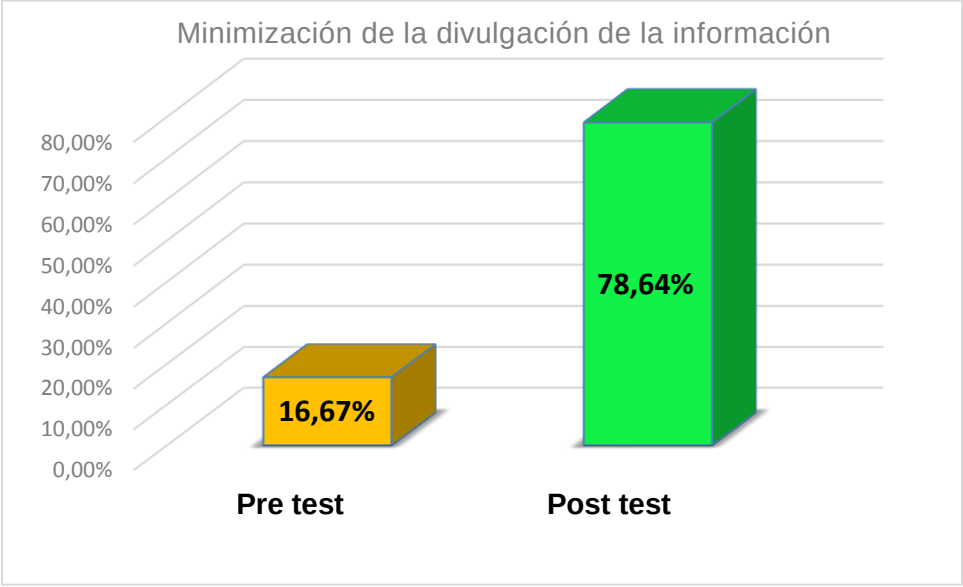


Gráfico 5. *Índice de la minimización de la divulgación de la información antes y después de la aplicación de MGSI*
Fuente: Elaboración propia

Interpretación: En el gráfico N°5, se observa el estado de la divulgación de la información minimizó significativamente en un 78.64% después de la aplicación del MGSI en la Municipalidad Distrital de Santa María de Chicmo, el 16.67% nos indica que la divulgación de la información es alta antes de la aplicación del MGSI.

b) Índice de minimización de alteración de la información antes y después de la aplicación del MGSI.

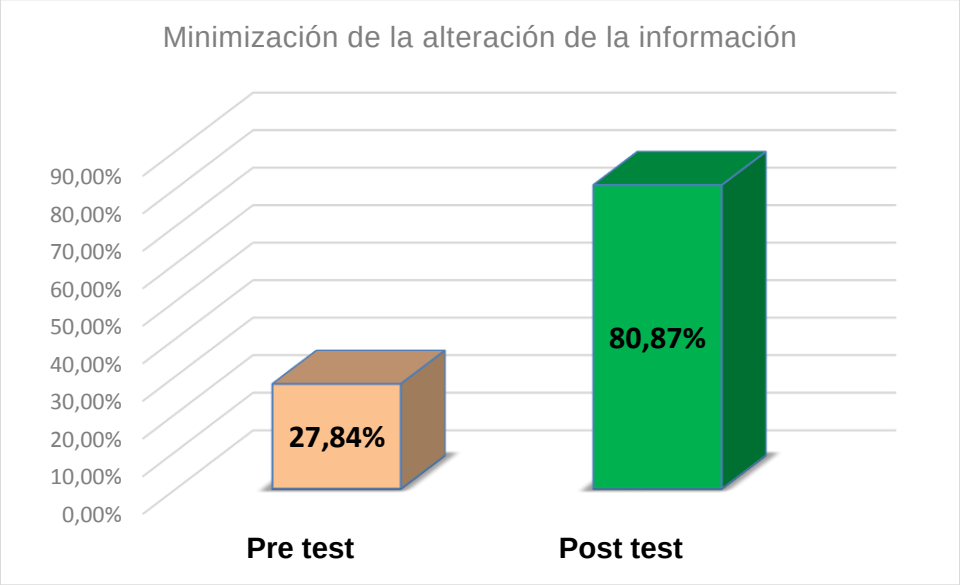


Gráfico 6. Índice de la minimización de la alteración de la información antes y después de la aplicación de MGSI
Fuente: Elaboración propia

Interpretación: En el gráfico N°6, se observa el estado de la alteración de la información minimizó significativamente en un 80.87% después de la aplicación de MGSI en la Municipalidad Distrital de Santa María de Chicmo, el 27.84% nos indica que la alteración de la información es alta antes de la aplicación del MGSI.

c) Índice de minimización de la amenazas de la información antes y después de la aplicación de MGSI.

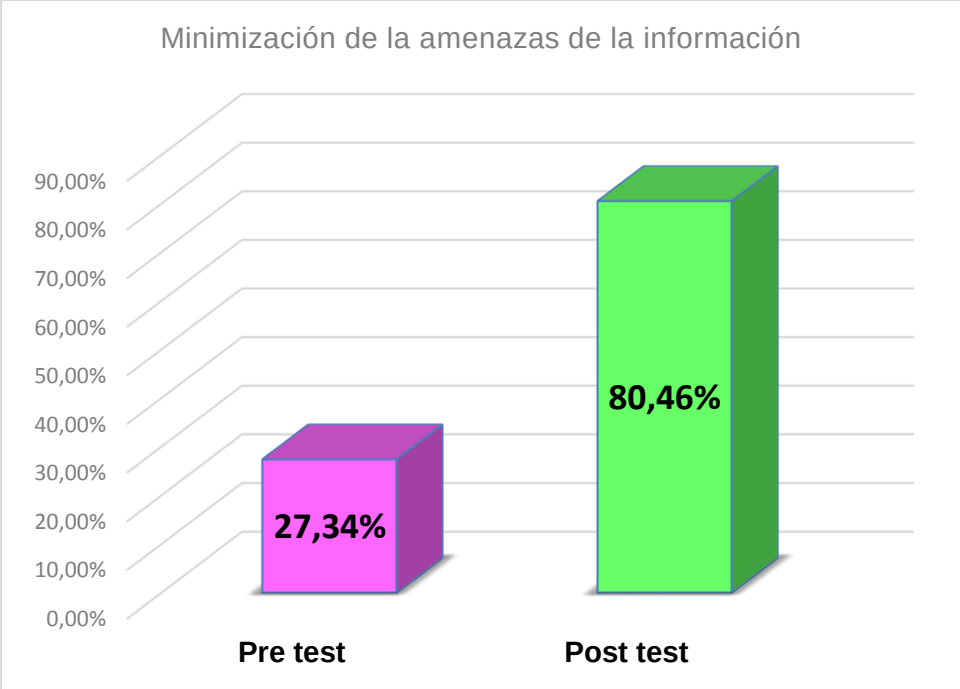


Gráfico 7. Índice de la minimización de la amenazas de la información antes y después de la aplicación de MGSI

Fuente: Elaboración propia

Interpretación: En el gráfico N°7, se observa el estado de la amenazas de la información minimizó significativamente en un 80,46% después de la aplicación de MGSI en la Municipalidad Distrital de Santa María de Chicmo, el 27,34% nos indica que la amenazas de la información es alta antes de la aplicación del MGSI.

d) Índice de minimización la vulnerabilidad de la información antes y después de la aplicación de MGSI.

Puntaje obtenido antes y después de aplicar el Modelo de Gestión de Seguridad de la Información para minimización de la vulnerabilidad de la información con ISO/IEC 27001 en la Municipalidad Distrital de Santa María de Chicmo Andahuaylas 2019 nos indica el siguiente gráfico Nº 8.

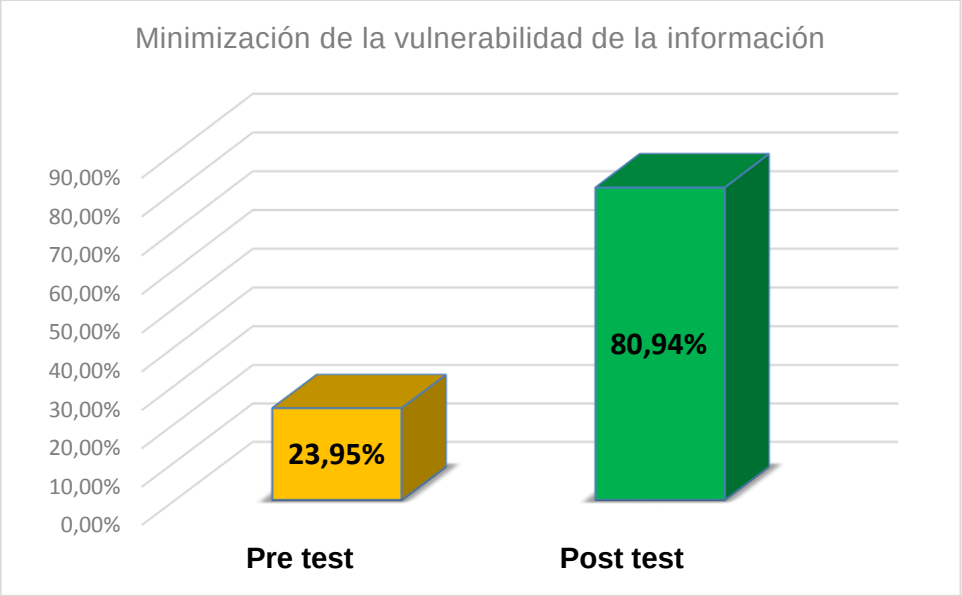


Gráfico 8. Índice de la minimización de la vulnerabilidad de la información antes y después de la aplicación de MGSI
Fuente: Elaboración propia

Interpretación: En el gráfico Nº8, se observa el estado de la vulnerabilidad de la información minimizó significativamente en un 80,94% después de la aplicación de MGSI en la Municipalidad Distrital de Santa María de Chicmo, el 23,95% nos indica que la vulnerabilidad de la información es alta antes de la aplicación del MGSI.

Dimensión	Puntaje pre test	Pre test	Puntaje post test	Post test	Variación porcentaje de minimización
Minimización Divulgación de la información	64	16,67%	302	78,64%	61,97%
Minimización alteración de la información	147	27,84%	427	80,87%	53,03%
Minimización amenazas de la información	105	27,34%	320	80,46%	53,12%
Minimización vulnerabilidad de la información	316	23,95%	1038	79,99%	56,04%

Tabla 9. *Verificación de porcentaje de la minimización de la vulnerabilidad de la información*
Fuente: elaboración propia

Interpretación: En la tabla N°9; se observa que, la variación en la minimización de la divulgación de la información es de 61,97%, quiere decir que minimizó la divulgación de la información muy significativamente, la variación de la minimización de alteración de la información es de 53,03%, quiere decir que disminuyó significativamente la alteración de la información, la variación de la minimización de amenazas de la información es de 53,12%, quiere decir que disminuyo significativamente la amenazas de la información, la variación de la minimización de la vulnerabilidad de la información con la aplicación del MGSI es de 56,04%, quiere decir que la minimización de la vulnerabilidad de la información es de significativo.

5.2 Prueba de hipótesis

Para comprobar la hipótesis de la investigación se ha utilizado la prueba de T-Student con un nivel de confianza de 95% y con nivel de significancia de 5%

Planteamiento de la hipótesis general

Hipótesis nula

H0: la vulnerabilidad de la información en la Municipalidad Distrital de Santa María de Chicmo no minimiza con la aplicación del MGSI

Hipótesis alternativa

H1: la vulnerabilidad de la información en la Municipalidad Distrital de Santa María de Chicmo si minimiza significativamente con la aplicación del MGSI

5.3 Verificación de la normalidad de los datos en SPSS

Comprobando la normalidad de los datos con una muestra pequeña de 24 terminales tecnológicos de la institución se considera el de Shapiro-Wilk donde:

H0: La pre y la post prueba no cumplen la distribución de la normalidad

H1: La pre y la post prueba cumplen la distribución de la normalidad

Si **P-valor** > 0,05, aceptamos H1.

Si **P-valor** < 0,05, rechazamos H1.

Pasando a determinar los datos en el software SPSS v24 se obtuvo la siguiente tabla de prueba de normalidad.

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PRE TEST	,138	23	,200*	,918	23	,053
POST TEST	,227	23	,002	,874	23	,006

Tabla 10. *Pruebas de Normalidad sobre la vulnerabilidad de la información*
Fuente: Elaborado en software SPSS

Interpretación: La tabla Nº 10, nos muestra que la significancia del pre test y post test es mayor que 0,05 por lo tanto se acepta la hipótesis alternativa por lo cual se afirma que los datos provienen de una distribución normal.

5.4 Aplicación de la prueba T-Student en muestras relacionadas

Los datos cumplen la distribución normal, por lo tanto a la seguida se procede a analizar los datos en prueba de t –Student para muestras relacionadas como indica lo siguiente:

Si **P-valor** > 0,05, aceptamos H0.

Si **P-valor** <= 0,05, aceptamos H1

Prueba de muestras emparejadas									
		Diferencias emparejadas							
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	PRE TEST – POST TEST	-30,08333	9,77093	1,99448	-34,20923	-25,95743	-15,083	23	,000

Tabla 11. *Prueba de muestras emparejadas sobre la vulnerabilidad de la información*

Fuente: Elaborado en software SPSS

Interpretación: En la tabla Nº 11, podemos observar el valor obtenido de **P-valor** (Sig. bilateral) es menor que 0,05 es decir que hay una diferencia significativa en la media de minimización de la vulnerabilidad de la información en la Municipalidad Distrital de santa María de Chicmo con la aplicación de MGSI.

Estadísticas de muestras emparejadas					
		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	PRE TEST	13,1667	24	6,77378	1,38269
	POST TEST	43,2500	24	4,42572	,90340

Tabla 12. *Estadísticas de muestras emparejadas general*

Fuente: Elaborado en software SPSS

Interpretación: Como se observa en la tabla Nº 12, la media del pre test es menor que la media de post test, entonces hay una diferencia entre los dos y eso nos indica que la aplicación del MGSI en la Municipalidad Distrital de santa María de Chicmo minimizó significativamente la vulnerabilidad de la información.

CAPÍTULO VI

DISCUSIÓN

En este estudio se realizó la comparación o la variación de la minimización de la vulnerabilidad de la información antes y después de la implementación del Modelo de Gestión de la Seguridad de la Información en la Municipalidad Distrital de Santa María de Chimo, donde se obtuvo como resultado 23,95% antes de la aplicación del MGSI el cual nos indica que la vulnerabilidad de la información es alta, la vulnerabilidad de la información minimizó en un 80,03% después de la aplicación del MGSI, quiere decir que los terminales tecnológicos de la municipalidad fueron implementados satisfactoriamente sobre la seguridad de la información, Vilca Mosquera (2017) el conocimiento sobre las políticas de seguridad en la empresa era mínimo antes de la aplicación, un 9.1% de la población solo tenía referencia de algunas normas laborales en cuanto al uso de los activos de la empresa, específicamente a las tecnologías de la información y comunicación, estas normas solo han sido mencionadas por los jefes de área o el gerente de la empresa, pero mas no habían sido plasmadas en un documento; ya posteriormente a la aplicación del SGSI se obtuvo que un 90,0% de la población ya tenía de conocimiento la existencia de una política de seguridad y que en si era un documento al cual se podía consultar ya que se realizaron reuniones de capacitación para dar a conocer todas las normas inmersas en la política de seguridad.

CONCLUSIONES

Con la prueba estadística T-Student y los resultados estadísticos, se llegó a comprobar que la implementación de Modelo de Gestión de la Seguridad de la Información con ISO/IEC 27001, da como resultado una variación positiva en la minimización la vulnerabilidad de la información en la Municipalidad Distrital de Santa María de Chicmo. Por lo tanto se concluye que hay una minimización de la vulnerabilidad de la información de manera significativa, ya que se determinó una variación positiva de 56,04% con respecto a la minimización de la vulnerabilidad de la información.

Con respecto a los trabajos realizados, con la implantación de MGSI para la minimización de la divulgación de la información en nuestro objeto de estudio, se determinó una variación positiva de 62,07%, lo cual nos indica que la divulgación de la información minimizó significativamente.

En la minimización de la alteración de la información con la implementación del MGSI se obtuvo un resultado significativo positivo de 53,03%, lo cual nos indica que la alteración de la información minimizó significativamente.

Por último, en la minimización de las amenazas de la información también se obtuvo una variación positiva de 53,12%, lo cual nos indica que la aplicación del MGSI para la minimización de las amenazas de la información es importante.

RECOMENDACIONES

Se recomienda a todas las empresas ya sean privada o pública a que puedan implantar un Sistema de Gestión de la Seguridad de la Información con ISO/IEC 27001 basada en buenas practicas, lo cual garantizará que su activo más importante este más confiable para la toma decisiones de las altas gerencias.

En esta institución, solo se implantó algunos controles de la seguridad de la información que son de prioridad para los trabajadores, por lo tanto, se recomienda implementar todos los controles con lo cual sería mucho mejor el cuidado del activo más valioso de la institución.

Se recomienda formar y capacitar de manera periódica a todos los personales de la institución, en temas de la seguridad de la información y así lograr que los activos más valiosos que tiene una institución esté integro, confiable y disponible.

La implantación del modelo de gestión de la seguridad de la información, en los terminales tecnológicos de una organización donde hay información vital debería estar en constante revisión, monitoreo y seguimiento de todos los controles que se tiene implementado.

REFERENCIAS BIBLIOGRÁFICAS

A. fauster, D. d. (2001). *Técnicas criptográficas de protección de datos.* España: Ra-Ma.

Aguilar Carrion , M. R. (2017). *Proyecto de Investigación Previa la Obtención del Grado.* Ambato, Ecuador.

Aguilera López, P. (2010). *Seguridad informática.* Malaga, España.

Aguirre Mollehuanca, D. A. (2014). *Diseño de un Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A.* Lima, Peru.

Amer, S, H., & Hamilton, J. A. (2008). *Understanding security architecture, in Proceedings of the.* ottawa, canada.

Areitio Bertolin, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* Madrid (España): Paraninfo.

Arévalo Moscoso, F. M. (2017). *Elaboracion y Plan de Implementacion de las Politicas de seguridad de la informacion Aplicadas a una Empresa Industrial de Alimentos.* Cuenca, Ecuador: Tesis de titulación de Magister en Gestión Estratégica de Tecnologías de la Información.

Aspectos claves de un SGSI basado en la norma ISO 27001 la norma ISO 27001. (2013, Octubre). *https://www.isotools.org*. Retrieved from Seguridad de la Informacion: https://www.isotools.org

Cabedo Semper, J. D., & Tirado Beltrán, J. M. (2009). *Divulgación de información sobre riesgos una propuesta para su medición.* españa.

Calder , A. (2007). *implementing Information Security based on ISO 27001 ISO 17799 – A Management Guide.*

Dussan clavijo, c. A. (2006). *Ciro Antonio Políticas de seguridad informática Entramado.* cali, colombia.

Firesmith, D. G. (2003). *Engineering Security Requirements. Journal of Object.*

Gandia Cabedo, J. L. (2002). *La divulgacion de la informacion sobre intangibles en el internet.* Valencia, España.

Hajdarević, K. (2013). *Proactive Information Security Metrics for Computer Network Architectures and Infrastructures, based on ISO 27001.* Sarajevo, Bosnia y Herzegovina.

Jimeno Martínez , M. G., & Maldonado Perez , D. D. (2013). *Propuesta de un Plan de Gestión del Riesgo para las Áreas De Almacén y Recepción de la Empresa ARP sura.* Barranquilla.

Legarda Muñoz, P. A., Lasso Garces, L. A., & Guerrero Erazo, H. A. (2015). *Identificación de Vulnerabilidades e Seguridad en el Control de Acceso al Sistema de Gestión Documental.* San Juan de Pasto .

Leiva Peña , R. (2015). *Diseño de un Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001 e ISO/IEC 27002.* Lambayeque.

Marcombo, A. (2007). *Diseño De Un Sistema De Seguridad Informática. Alfa omega.* Mexico.

Mantilla Guerra , A. R. (2009). *Diseño de un Sistema de Gestion de la Seguridad de la Informacion para cooperativa ahorro y credito basada en la norma ISO/IEC 27001.* Quito, Ecuador.

Marc Royer, J. (2004). *Seguridad en la Informatica de Empresa: Riesgos, Amenazas, Prevencion y Soluciones.* Barcelona.

Neubauer, T., Ekelhart, A., & Fenz, S. (2008). *Interactive Selection of ISO 27001 Controls.* Austria.

R. Peltier, T. (2005). *Informacion Security Risk Analisys.* New York.

Rico Bautista, D. W., Arévalo Ascanio, J. G., & Bayona Trillos, R. A. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001. *Tecnura*, 12.

Roberto Hernández Sampieri, C. F. (2014). *Metodologia de la investigacion* . Mexico: Quinta edicion .

Sanchez Arias, K. (2014). *Diseño de Políticas de Seguridad de Información para la Alcaldía Municipal de Rio de Oro, Cesar.* Ocaña, Colombia.

Sistema de gestion de la seguridad de la informacion. (2013, Marzo). *iso 27001*. Retrieved from WWW.iso27000.es

Sistema de Gestion de la Seguridad de la Informacion. (2013, octubre). *WWW.iso27000.es*.

Solarte Solarte, F. N., Enriquez Rosero, E. R., & Benavides Ruano, M. (2015). *Methodology of analysis and risk assessment applied to computer security and information under the ISO / IEC 27001.* Colombia.

Susanto, h., Mohammad Nabil Almunawar, M., & Chee , Y. (2012). Information Security Challenge and Breaches: Novelty Approach on Measuring ISO 27001 Readiness Level.

Talavera Alvarez , V. R. (2015). *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.* Lima.

Tarazona T., C. H. (2013). *Amenazas Informáticas y Seguridad de da Información.* Colombia.

ANEXO 1: Matriz de Consistencia

"MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON ISO/IEC 27001 PARA MINIMIZAR LA VULNERABILIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE SANTA MARÍA DE CHICMO – ANDAHUAYLAS-2018"						
PROBLEMA	**OBJETIVO**	**HIPOTESIS**	**VARIABLE**	**DIMENSION**	**INDICADORES**	**METODOLOGÍA**
General ¿En qué medida el Modelo de Gestión de la Seguridad de la Información con ISO/IEC 27001 minimizará la vulnerabilidad de la información en la Municipalidad Distrital de Santa María de Chicmo-Andahuaylas-2018?	**General** Minimizar la vulnerabilidad de la información a través del Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001 en la Municipalidad Distrital de Santa María de Chicmo – Andahuaylas-2018	**General** El Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001 minimizará la vulnerabilidad de la información en la Municipalidad Distrital de Santa María de Chicmo – Andahuaylas-2018	**V. Independiente** Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001			Método (cuantitativo) Nivel (explicativo) Diseño (pre experimental).
¿En qué medida el Modelo de Gestión de la Seguridad de la Información con ISO/IEC 27001 minimizará la divulgación de la información en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas-2018?	Minimizar la divulgación de la información a través del Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001 en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas-2018	El Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001 minimizara la divulgación de la información en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas-2018	**V. Dependiente** Minimizar la vulnerabilidad de la información	Divulgación de la información	% de la minimización de la divulgación de la información.	Población: los 24 terminales tecnológico de la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas. Muestra: los 24 terminales tecnológicos de la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas.
¿En qué medida el Modelo de Gestión de la Seguridad de la Información con ISO/IEC 27001 minimizará la alteración de la información en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas-2018?	Minimizar la alteración de la información a través del Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001 en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas-2018	El Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001 minimizara la alteración de la información en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas-2018		Alteración de la información	% de la minimización de Alteración de la información.	
¿En qué medida el Modelo de Gestión de la Seguridad de la Información con ISO/IEC 27001 minimizará la amenaza de la información en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas-2018?	Minimizar la amenazas de la información a través del Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001 en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas-2018	El Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001 minimizara la amenaza de la información en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas-2018		Amenazas de la información	% de la minimización de Amenazas de la información	

ANEXO 2. Lista de cotejo sobre la Seguridad de la Información

Buenas tardes, Sr.(a) soy…… , Estamos realizando un estudio sobre el Proyecto de "**MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON ISO/IEC 27001 PARA MINIMIZAR LA VULNERABILIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE SANTA MARÍA DE CHICMO – ANDAHUAYLAS" Apurímac 2019**.

Por tal motivo, me gustaría revisar los su terminal tecnológico. La información que nos levantada será estrictamente confidencial y permanecerá en absoluta reserva. Según Ley Nº 29733 (Ley de Protección de Datos Personales).

¿Puedo iniciar el trabajo ahora?

Acepta ◯ En otro momento ◯ No acepta la entrevista ◯ Fecha: ___/___/2019 N° de Encuesta ☐

I DIVULGACION DE LA INFORMACIÓN

1.1. ¿Los terminales de la municipalidad cuenta con políticas de la seguridad de la información?

NO ( ) PARCIALMENTE ( ) SI ( )

1.2. ¿La Municipalidad le hizo conocer las políticas de seguridad de la información de los terminales tecnológicos?

NO ( ) PARCIALMENTE ( ) SI ( )

1.3. ¿Algún encargado de terminal tecnológico fue capacitado sobre la seguridad de la información por un especialista de la Municipalidad o una empresa especializada?

NO ( ) PARCIALMENTE ( ) SI ( )

1.4. ¿Se utiliza algún medio de seguridad para enviar información referida a la municipalidad a través de las computadora y/o dispositivo móvil? ejemplo patrón seguro

NO ( ) PARCIALMENTE ( ) SI ( )

1.5. ¿La dirección exige a tener en cuenta la Seguridad de la Información para el uso de los terminales?

NO ( ) PARCIALMENTE ( ) SI ( )

1.6. ¿La información es confidencial en los terminales tecnológicos?

NO ( ) PARCIALMENTE ( ) SI ( )

1.7. ¿Existe control adecuada de la salida de los terminales tecnológicos de la municipalidad?

NO ( ) PARCIALMENTE ( ) SI ( )

1.8. ¿La contraseña del terminal tecnológico es confidencial?

NO ( ) PARCIALMENTE ( ) SI ( )

II ALTERACIÓN DE LA INFORMACIÓN

2.1. ¿La información es manipulada de acuerdo a dónde pertenece o corresponde?

NO ( ) PARCIALMENTE ( ) SI ( )

2.2. ¿La institución cuenta con una política de control de accesos a las áreas donde hay equipos tecnológicos?

NO ( ) PARCIALMENTE ( ) SI ( )

2.3. ¿Las computadoras y dispositivos móviles cuenta con una contraseña seguro para permitir el acceso?

NO ( ) PARCIALMENTE ( ) SI ( )

2.4. ¿Ud. Revisa la conformidad de toda la información que tiene en su computadora y dispositivos móviles con frecuencia?

NO ( ) PARCIALMENTE ( ) SI ( )

2.5. ¿La contraseña de acceso de usuarios es cambiada frecuentemente?

NO ( ) PARCIALMENTE ( ) SI ( )

2.6. ¿Se utiliza mecanismos de bloqueo automático de su computadora personal cuando se deja de usar?

NO ( ) PARCIALMENTE ( ) SI ( )

2.7. ¿Las contraseñas de acceso de usuario a las computadoras donde se tiene información vital son descifradas o combinados con caracteres?

NO ( ) PARCIALMENTE ( ) SI ( )

2.8. ¿Se asegura que las computadoras donde trabaja cuenten con protección adecuada contra virus informático?

NO ( ) PARCIALMENTE ( ) SI ( )

2.9. ¿Las computadoras donde se labora tienen instalado antivirus?

NO ( ) PARCIALMENTE ( ) SI ( )

2.10. ¿La información está protegida contra posibles alteraciones?

NO ( ) PARCIALMENTE ( ) SI ( )

2.11. ¿Se restringen la instalación de otras aplicaciones o software que no sea de trabajo?

NO ( ) PARCIALMENTE ( ) SI ( )

III AMENAZAS DE LA INFORMACIÓN

3.1. ¿La municipalidad cuenta con controles de acceso al personal de la institución y público en general?

NO ( ) PARCIALMENTE ( ) SI ( )

3.2. ¿La puerta y las ventanas de las áreas de trabajo se encuentran segura?

NO ( ) PARCIALMENTE ( ) SI ( )

3.3. ¿La computadora es laborado solo por personal autorizado?

NO ( ) PARCIALMENTE ( ) SI ( )

3.4. El área de trabajo está bien ubicado y seguro contra amenazas externas? Ejemplo inundaciones

NO ( ) PARCIALMENTE ( ) SI ( )

3.5. ¿En caso de alguna falla del internet en su computadora y/o dispositivo móvil Ud. conoce donde ir para su pronta verificación?

NO ( ) PARCIALMENTE ( ) SI ( )

3.6. ¿Se realiza mantenimiento periódico del hardware y software en la institución?

NO ( ) PARCIALMENTE ( ) SI ( )

3.7. ¿Se realiza copias de la información que manejada en el equipo tecnológico de trabajo?

NO ( ) PARCIALMENTE ( ) SI ( )

3.8. ¿La institución cuenta con un personal responsable sobre seguridad de la información?

NO ( ) PARCIALMENTE ( ) SI ( )

Buenas tardes, Sr.(a) soy..... Yover Huamán Atacco ..... , Estamos realizando un estudio sobre el Proyecto de **"MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON ISO/IEC 27001 PARA MINIMIZAR LA VULNERABILIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE SANTA MARIA DE CHICMO – ANDAHUAYLAS" Apurímac 2019**. Por tal motivo, me gustaría revisar los su terminal tecnológico. La información que nos levantada será estrictamente confidencial y permanecerá en absoluta reserva. Según Ley Nº 29733 (Ley de Protección de Datos Personales).

¿Puedo iniciar el trabajo ahora?

Acepta ◯ En otro momento ◯ No acepta la entrevista ◯ Fecha: 22/02/ 2019 N° de Encuesta 19

I DIVULGACION DE LA INFORMACIÓN

1.1. ¿Los terminales de la municipalidad cuenta con políticas de la seguridad de la información?

NO ( ) PARCIALMENTE ( ) SI (X)

1.2. ¿La Municipalidad le hizo conocer las políticas de seguridad de la información de los terminales tecnológicos?

NO ( ) PARCIALMENTE ( ) SI (X)

1.3. ¿Algún encargado de terminal tecnológico fue capacitado sobre la seguridad de la información por un especialista de la Municipalidad o una empresa especializada?

NO ( ) PARCIALMENTE ( ) SI (X)

1.4. ¿Se utiliza algún medio de seguridad para enviar información referida a la municipalidad a través de las computadora y/o dispositivo móvil? ejemplo patrón seguro

NO ( ) PARCIALMENTE ( ) SI (X)

1.5. ¿La dirección exige a tener en cuenta la Seguridad de la Información para el uso de los terminales?

NO ( ) PARCIALMENTE ( ) SI (X)

1.6. ¿La información es confidencial en los terminales tecnológicos?

NO ( ) PARCIALMENTE (X) SI ( )

1.7. ¿Existe control adecuada de la salida de los terminales tecnológicos de la municipalidad?

NO ( ) PARCIALMENTE ( ) SI (X)

1.8. ¿La contraseña del terminal tecnológico es confidencial?

NO ( ) PARCIALMENTE ( ) SI (X)

II ALTERACIÓN DE LA INFORMACIÓN

2.1. ¿La información es manipulada de acuerdo a dónde pertenece o corresponde?

NO ( ) PARCIALMENTE ( ) SI (X)

2.2. ¿La institución cuenta con una política de control de accesos a las áreas donde hay equipos tecnológicos?

NO ( ) PARCIALMENTE ( ) SI (X)

2.3. ¿Las computadoras y dispositivos móviles cuenta con una contraseña seguro para permitir el acceso?

NO ( ) PARCIALMENTE ( ) SI (X)

2.4. ¿Ud. Revisa la conformidad de toda la información que tiene en su computadora y dispositivos móviles con frecuencia?

NO ( ) PARCIALMENTE ( ) SI (X)

2.5. ¿La contraseña de acceso de usuarios es cambiada frecuentemente?

NO ( ) PARCIALMENTE ( ) SI (X)

2.6. ¿Se utiliza mecanismos de bloqueo automático de su computadora personal cuando se deja de usar?

NO ( ) PARCIALMENTE ( ) SI (X)

2.7. ¿Las contraseñas de acceso de usuario a las computadoras donde se tiene información vital son descifradas o combinados con caracteres?

NO ( ) PARCIALMENTE (X) SI ( )

2.8. ¿Se asegura que las computadoras donde trabaja cuenten con protección adecuada contra virus informático?

NO ( ) PARCIALMENTE (X) SI ( )

2.9. ¿Las computadoras donde se labora tienen instalado antivirus?

NO ( ) PARCIALMENTE ( ) SI (X)

2.10. ¿La información está protegida contra posibles alteraciones?

NO ( ) PARCIALMENTE ( ) SI (X)

2.11. ¿Se restringen la instalación de otras aplicaciones o software que no sea de trabajo?

NO (X) PARCIALMENTE ( ) SI ( )

III AMENAZAS DE LA INFORMACIÓN

3.1. ¿La municipalidad cuenta con controles de acceso al personal de la institución y público en general?

NO ( ) PARCIALMENTE ( ) SI (X)

3.2. ¿La puerta y las ventanas de las áreas de trabajo se encuentran segura?

NO ( ) PARCIALMENTE (X) SI ( )

3.3. ¿La computadora es laborado solo por personal autorizado?

NO ( ) PARCIALMENTE ( ) SI (X)

3.4. ¿El área de trabajo está bien ubicado y seguro contra amenazas externas? Ejemplo inundaciones

NO ( ) PARCIALMENTE ( ) SI (X)

3.5. ¿En caso de alguna falla del internet en su computadora y/o dispositivo móvil Ud. conoce donde ir para su pronta verificación?

NO ( ) PARCIALMENTE (X) SI ( )

3.6. ¿Se realiza mantenimiento periódico del hardware y software en la institución?

NO ( ) PARCIALMENTE ( ) SI (X)

3.7. ¿Se realiza copias de la información que manejada en el equipo tecnológico de trabajo?

NO ( ) PARCIALMENTE ( ) SI (X)

3.8. ¿La institución cuenta con un personal responsable sobre seguridad de la información?

NO ( ) PARCIALMENTE ( ) SI (X)

Buenas tardes, Sr.(a) soy..... Javier Huaman Ancco ..... , Estamos realizando un estudio sobre el Proyecto de **"MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON ISO/IEC 27001 PARA MINIMIZAR LA VULNERABILIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE SANTA MARIA DE CHICMO – ANDAHUAYLAS" Apurímac 2019**. Por tal motivo, me gustaría revisar los su terminal tecnológico. La información que nos levantada será estrictamente confidencial y permanecerá en absoluta reserva. Según Ley Nº 29733 (Ley de Protección de Datos Personales).

¿Puedo iniciar el trabajo ahora?

Acepta (X) En otro momento ( ) No acepta la entrevista ( ) Fecha: 21/ 08/ 2019 N° de Encuesta 01

I DIVULGACION DE LA INFORMACIÓN

1.1. ¿Los terminales de la municipalidad cuenta con políticas de la seguridad de la información?

NO ( ) PARCIALMENTE ( ) SI (X)

1.2. ¿La Municipalidad le hizo conocer las políticas de seguridad de la información de los terminales tecnológicos?

NO ( ) PARCIALMENTE ( ) SI (X)

1.3. ¿Algún encargado de terminal tecnológico fue capacitado sobre la seguridad de la información por un especialista de la Municipalidad o una empresa especializada?

NO ( ) PARCIALMENTE ( ) SI (X)

1.4. ¿Se utiliza algún medio de seguridad para enviar información referida a la municipalidad a través de las computadora y/o dispositivo móvil? ejemplo patrón seguro

NO ( ) PARCIALMENTE ( ) SI (X)

1.5. ¿La dirección exige a tener en cuenta la Seguridad de la Información para el uso de los terminales?

NO ( ) PARCIALMENTE ( ) SI (X)

1.6. ¿La información es confidencial en los terminales tecnológicos?

NO ( ) PARCIALMENTE (X) SI ( )

1.7. ¿Existe control adecuada de la salida de los terminales tecnológicos de la municipalidad?

NO ( ) PARCIALMENTE (X) SI ( )

1.8. ¿La contraseña del terminal tecnológico es confidencial?

NO ( ) PARCIALMENTE ( ) SI (X)

II ALTERACIÓN DE LA INFORMACIÓN

2.1. ¿La información es manipulada de acuerdo a dónde pertenece o corresponde?

NO ( ) PARCIALMENTE ( ) SI (X)

2.2. ¿La institución cuenta con una política de control de accesos a las áreas donde hay equipos tecnológicos?

NO ( ) PARCIALMENTE (X) SI ( )

2.3. ¿Las computadoras y dispositivos móviles cuenta con una contraseña seguro para permitir el acceso?

NO ( ) PARCIALMENTE ( ) SI (X)

2.4. ¿Ud. Revisa la conformidad de toda la información que tiene en su computadora y dispositivos móviles con frecuencia?

NO ( ) PARCIALMENTE (X) SI ( )

2.5. ¿La contraseña de acceso de usuarios es cambiada frecuentemente?

NO ( ) PARCIALMENTE ( ) SI (X)

2.6. ¿Se utiliza mecanismos de bloqueo automático de su computadora personal cuando se deja de usar?

NO ( ) PARCIALMENTE ( ) SI (X)

2.7. ¿Las contraseñas de acceso de usuario a las computadoras donde se tiene información vital son descifradas o combinados con caracteres?

NO ( ) PARCIALMENTE ( ) SI (X)

2.8. ¿Se asegura que las computadoras donde trabaja cuenten con protección adecuada contra virus informático?

NO ( ) PARCIALMENTE (X) SI ( )

2.9. ¿Las computadoras donde se labora tienen instalado antivirus?

NO ( ) PARCIALMENTE ( ) SI (X)

2.10. ¿La información está protegida contra posibles alteraciones?

NO ( ) PARCIALMENTE ( ) SI (X)

2.11. ¿Se restringen la instalación de otras aplicaciones o software que no sea de trabajo?

NO ( ) PARCIALMENTE ( ) SI (X)

III AMENAZAS DE LA INFORMACIÓN

3.1. ¿La municipalidad cuenta con controles de acceso al personal de la institución y público en general?

NO ( ) PARCIALMENTE ( ) SI (X)

3.2. ¿La puerta y las ventanas de las áreas de trabajo se encuentran segura?

NO ( ) PARCIALMENTE ( ) SI (X)

3.3. ¿La computadora es laborado solo por personal autorizado?

NO ( ) PARCIALMENTE (X) SI ( )

3.4. ¿El área de trabajo está bien ubicado y seguro contra amenazas externas? Ejemplo inundaciones

NO ( ) PARCIALMENTE (X) SI ( )

3.5. ¿En caso de alguna falla del internet en su computadora y/o dispositivo móvil Ud. conoce donde ir para su pronta verificación?

NO ( ) PARCIALMENTE ( ) SI (X)

3.6. ¿Se realiza mantenimiento periódico del hardware y software en la institución?

NO ( ) PARCIALMENTE ( ) SI (X)

3.7. ¿Se realiza copias de la información que manejada en el equipo tecnológico de trabajo?

NO ( ) PARCIALMENTE ( ) SI (X)

3.8. ¿La institución cuenta con un personal responsable sobre seguridad de la información?

NO ( ) PARCIALMENTE ( ) SI (X)

ANEXO 3. Validación de instrumento de investigación

CONSTANCIA DE VALIDACIÓN

Quien suscribe, Enrique Edgardo Condor Tinoco,
Con documento de identidad Nº 40998311, de profesión ing. de sistemas
con Grado de _____, ejerciendo actualmente como Docente,
en la Institución Universidad Nacional José María Arguedas.
Por medio de la presente hago constar que he revisado con fines de Validación el Instrumento (encuesta), a los efectos de su aplicación en la Municipalidad Distrital de Santa María de Chicmo Provincia Andahuaylas

Luego de hacer las observaciones pertinentes, puedo formular las siguientes Apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	EXCELENTE
Congruencia de Ítems			X	
Amplitud de contenido				X
Redacción de los Ítems			X	
Claridad y precisión				X
Pertinencia				X

Andahuaylas 13 de diciembre del año 2018

UNIVERSIDAD NACIONAL JOSE MARIA ARGUEDAS
Ing. Enrique Edgardo Condor Tinoco
DOCENTE

Firma
DNI n°.40998311

CONSTANCIA DE VALIDACIÓN

Quien suscribe, JUAN José Oré Cerrón,

Con documento de identidad Nº 20443907, de profesión _____ con Grado de Maestro en Ing. Sistemas ejerciendo actualmente como DOCENTE, en la Institución Universidad Nacional José María Arguedas.

Por medio de la presente hago constar que he revisado con fines de Validación el Instrumento (encuesta), a los efectos de su aplicación en la Municipalidad Distrital de Santa María de Chicmo Provincia Andahuaylas

Luego de hacer las observaciones pertinentes, puedo formular las siguientes Apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	EXCELENTE
Congruencia de Ítems				X
Amplitud de contenido			X	
Redacción de los Ítems				X
Claridad y precisión			X	
Pertinencia				X

Andahuaylas 19 de diciembre del año 2018

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS
Ing. Juan José Oré Cerrón
DOCENTE

Firma
DNI nº 20443907

CONSTANCIA DE VALIDACIÓN

Quien suscribe, Jovana Flores Ccorisapra,

Con documento de identidad Nº 45889868, de profesión Ing. Informatico y Sistemas con Grado de Ingeniero,

ejerciendo actualmente como Jefe, en la Institución Universidad Nacional José María Arguedas.

Por medio de la presente hago constar que he revisado con fines de Validación el Instrumento (encuesta), a los efectos de su aplicación en la Municipalidad Distrital de Santa María de Chicmo Provincia Andahuaylas

Luego de hacer las observaciones pertinentes, puedo formular las siguientes Apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	EXCELENTE
Congruencia de Ítems				X
Amplitud de contenido				X
Redacción de los Ítems				X
Claridad y precisión				X
Pertinencia			X	

Andahuaylas 19 de diciembre del año 2018

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS
Ing. Jovana Flores Ccorisapra
JEFE (E) DE LA UNIDAD DE SISTEMAS DE INFORMACIÓN

Firma
DNI n°. 45889868

ANEXO 4. Solicitud de permiso para realizar trabajos de investigación

"AÑO DE LA LUCHA CONTRA LA CORRUPCIÓN E IMPUNIDAD"

SOLICITO: permiso para encuesta personal de la municipalidad

Santa María de Chicmo 16 de enero del 2019

SEÑOR: MAX RAFAEL HUARACA PARIONA
ALCALDE DE LA MUNICIPALIDAD DISTRITAL DE SANTA MARÍA DE CHICMO

MUNICIPALIDAD DISTRITAL SANTA MARÍA DE CHICMO
MESA DE PARTES
16 ENE. 2019
Reg. N° 198 Hora: 2:33
Folio: 01 Firma:

Yo Yuver Huamán Ancco identificado con DNI N°46008673 domiciliado en centro poblado de Rebelde Huayrana Distrito De Santa María De Chicmo Provincia Andahuaylas ante Ud. con el debido respeto me presento y digo

Que teniendo la oportunidad de saludarle muy cordialmente y a la vez solicitarle permiso de ingreso a la municipalidad principalmente su tiempo de cada trabajador de todas las áreas par realizar una encuesta del proyecto titulado "MODELO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CON ISO/IEC 27001 PARA MINIMIZAR LA VULNERABILIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE SANTA MARÍA DE CHIMO , ANDAHUAYLAS 2019" aprobado por la Universidad Nacional José María Arguedas, esta encuesta será valioso, vital para el interesado y el principal beneficiado con este proyecto será la institución, los resultados obtenidos ayudaran significativamente a la alta gerencia en la toma de decisiones.

Por lo expuesto.

Agradezco anticipadamente la atención que brinda a esta solicitud.

Atentamente.

Yuver Huamán Ancco
46008673

Publicación de políticas de Seguridad de la Información

Gestión 2019-2022

MUNICIPALIDAD DISTRITAL DE SANTA MARÍA DE CHICMO
"AÑO DE LA LUCHA CONTRA LA CORRUPCION E IMPUNIDAD"

Comunicado Aprobación del Modelo de Gestión de la Seguridad de la Información

Quien suscribe Ing. Virgilio Sánchez Rojas con documento de identidad Nº 31184618, Gerente de la Municipalidad distrital de Santa María de Chicmo, Provincia Andahuaylas, Región Apurímac.

El presente documento hago constar con fines de aprobar la elaboración del Modelo de Gestión de la Seguridad de la Información para la minimización de vulnerabilidad de la información lo cual fue aplicada a nuestra institución por un especialista del tema. El trabajador deberá cumplir de manera urgente las políticas aprobadas por la gerencia.

Santa María de Chicmo 01 de febrero del año 2019

MUNICIPALIDAD DISTRITAL DE SANTA MARIA DE CHICMO
Ing. Virgilio Sánchez Rojas
GERENTE MUNICIPAL

Citación para la capacitación a los trabajadores de la municipalidad

Gestión 2019-2022

MUNICIPALIDAD DISTRITAL DE SANTA MARÍA DE CHICMO
"AÑO DE LA LUCHA CONTRA LA CORRUPCION E IMPUNIDAD"

Un Gobierno Para Todos...!

TRABAJADORES DE MUNICIPALIDAD DE "CHICMO" RECIBEN CAPACITACION SOBRE LA SEGURIDAD DE LA INFORMACIÓN

La Municipalidad distrital de santa María de Chicmo, atreves de jefe de recursos humanos, convoca a una charla que se llevara a cabo sobre la seguridad de la información el día 08 de febrero a las 4:00 pm del 2019.

Por encargo del señor José Leguía Ortega jefe de recursos humanos se hizo posible convocar y brindar capacitación que permitirán impulsar la seguridad de la información y reavivar los principios y valores en los trabajadores de la municipalidad.

"Esta capacitación tiene como finalidad sensibilizar a todos los trabajadores de la municipalidad y población asistente" dijo el especialista sobre la seguridad de la información el Sr. Yuver Huamán Ancco, quien agradeció al "alcalde" por preocuparse en la seguridad del activo más valioso de la institución que es la información.

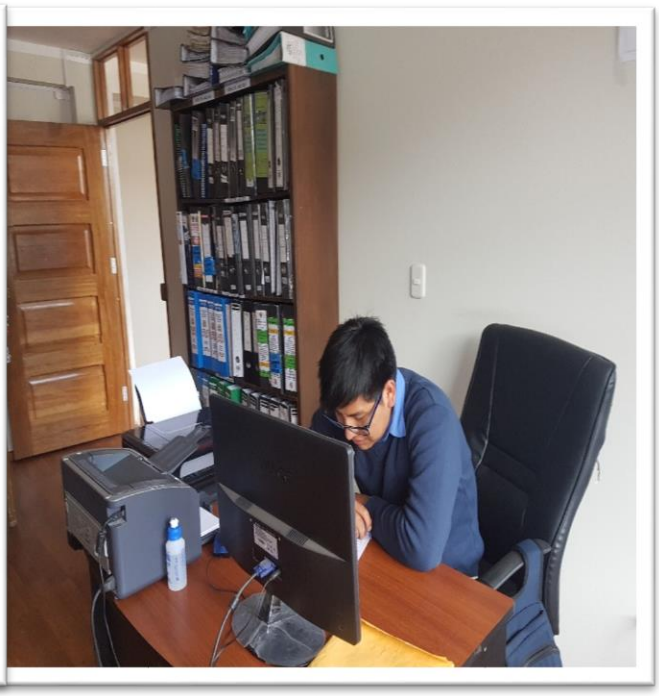
Cabe señalar que la Municipalidad de Chicmo, viene realizando nuevos planes estratégicos en favor de la seguridad de la información en coordinación con el especialista, para llevar en tranquilidad la información que cada trabajador maneja en su terminal tecnológico.

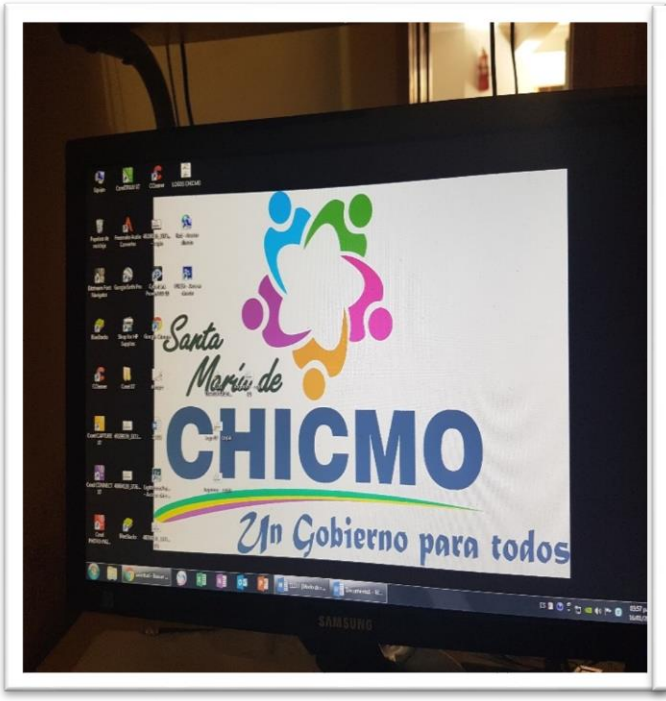
Santa María de Chicmo, 04 de febrero del 2019

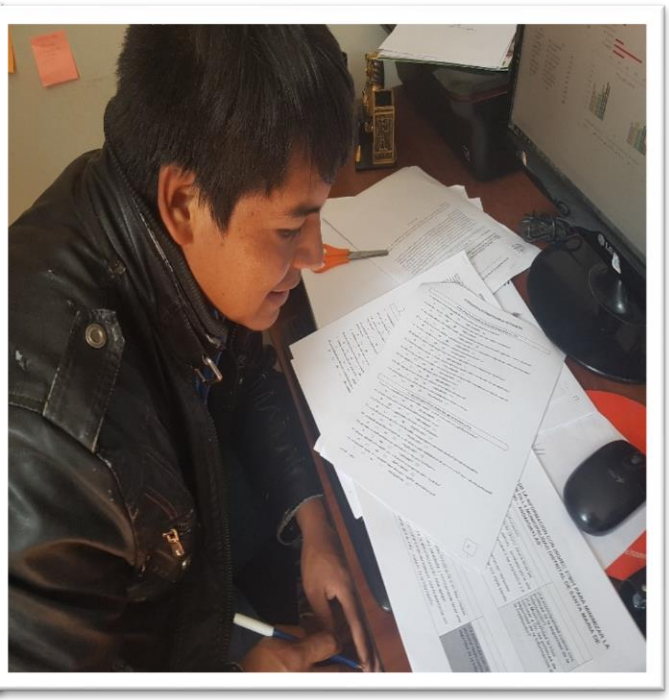
MUNICIPALIDAD DISTRITAL SANTA MARIA DE CHICMO
José Alejandro Leguía Ortega
JEFE DE PERSONAL

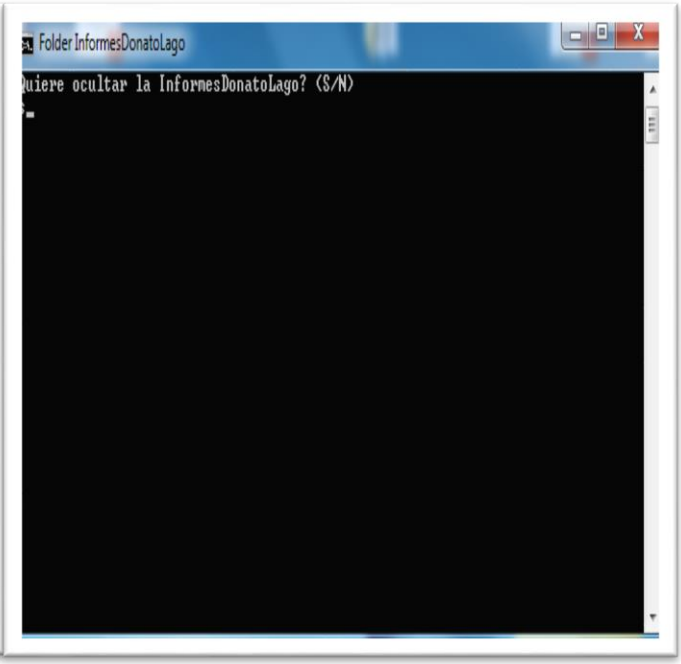
Dirección: Jr. Tupac Amaru Nª 202 Plaza de Armas
web. http. //www. Munisantamariadechicmo.gob.pe **E-mail:** info: munichicmo2019@gmail.com

ANEXO 5. Fotografías realizando el pre test y post test








Folder InformesDonatoLago
Quiere ocultar la InformesDonatoLago? (S/N)


Las Normas de Seguridad de la Información

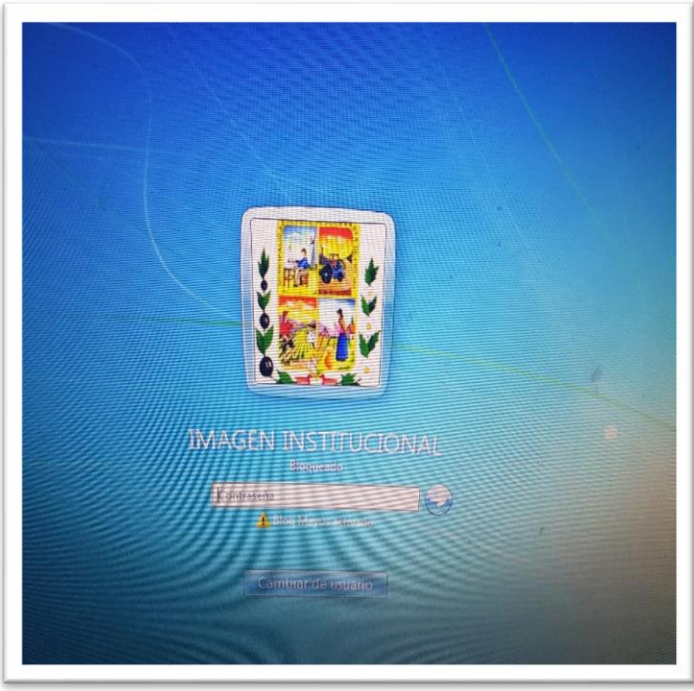
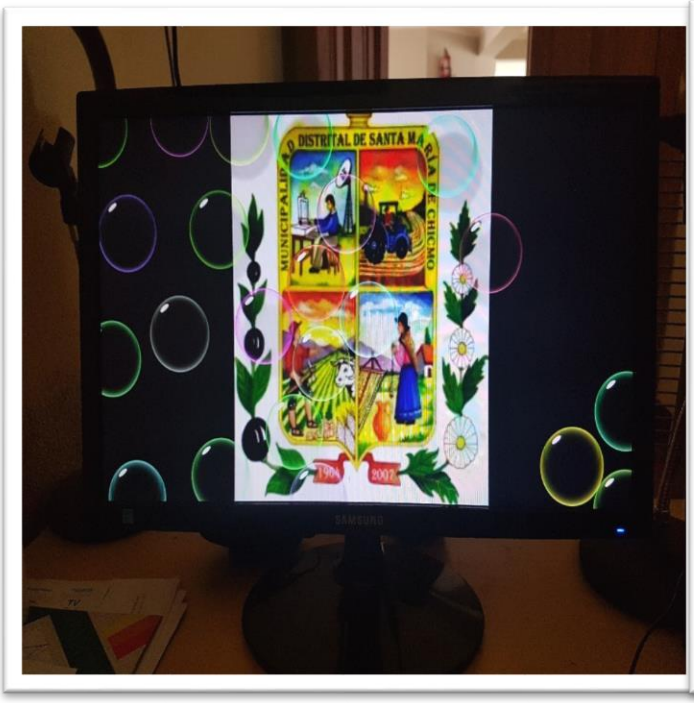
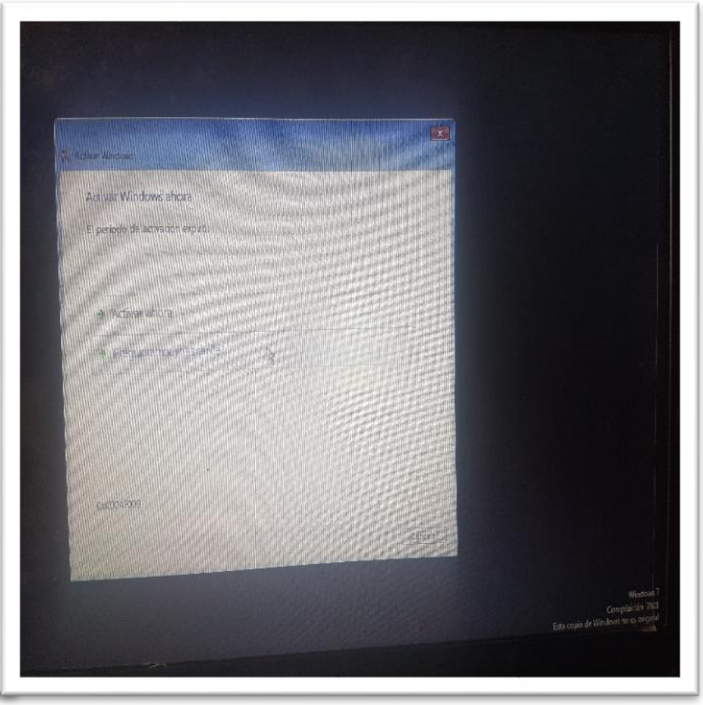


IMAGEN INSTITUCIONAL
Bloqueado
Cambiar de usuario


Yale
10:39


MUNICIPALIDAD DISTRITAL DE SANTA MARIA DEL CHICMO
1904
2007


Activar Windows ahora
El periodo de activación expiró.