UNIVERSIDAD CATÓLICA ÁNGELES CHIMBOTE

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE SISTEMAS

PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON NORMAS ISO 27001 PARA LA MUNICIPALIDAD DISTRITAL DE BUENA VISTA ALTA – CASMA; 2017.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR

COLONIA HERNÁNDEZ, PEDRO JESÚS
ORCID: 0000-0001-7705-8663

ASESOR

SUXE RAMÍREZ, MARÍA ALICIA
ORCID: 0000-0002-1358-4290

CHIMBOTE – PERÚ

2019

EQUIPO DE TRABAJO

AUTOR

Colonia Hernández, Pedro Jesús

ORCID: 0000-0003-8970-5629

Universidad Católica Los Ángeles de Chimbote, Estudiante de Pregrado, Chimbote, Perú

ASESOR

Suxe Ramírez, María Alicia

ORCID: 0000-0002-1358-4290

Universidad Católica Los Ángeles de Chimbote, Facultad de Ingeniería, Escuela Profesional de Sistemas, Chimbote, Perú

JURADO

Castro Curay, José Alberto

ORCID ID:0000-0003-0794-2968

Ocaña Velásquez, Jesús Daniel

ORCID ID: 0000-0002-1671- 429X

Torres Ceclén, Carmen Cecilia

ORCID ID: 0000-0002-8616-7965

JURADO EVALUADOR DE TESIS Y ASESOR

MGTR. ING. CIP. JOSÉ ALBERTO CASTRO CURAY
PRESIDENTE

MGTR. ING. CIP. JESÚS DANIEL OCAÑA VELÁSQUEZ
MIEMBRO

MGTR. ING. CIP. CARMEN CECILIA TORRES CECLÉN
MIEMBRO

DRA. ING. CIP. MARÍA ALICIA SUXE RAMÍREZ
ASESOR

DEDICATORIA

A mis padres, Medali y Pedro, porque siempre estuvieron de mi lado, me dieron su apoyo y sus consejos para hacerme una mejor persona.

A mi hermana, Keiko, gracias por estar conmigo y apoyarme siempre, la quiero mucho.

A mis abuelos, Alfonsa y Máximo, quienes, para mi persona, fueron un gran ejemplo de perseverancia, trabajo y esfuerzo.

Pedro Jesús Colonia Hernández

AGRADECIMIENTO

A Dios por permitirme tener y disfrutar a mi familia, gracias a mi familia por apoyarme en cada decisión y proyecto, a la vida porque cada día me demuestra lo hermoso que es la vida y lo justo que puede llegar a ser; gracias a mi familia por permitir cumplir con excelencia en el desarrollo de esta tesis, Gracias por creer en mí y gracias a Dios por permitirme vivir y disfrutar cada día.

A mi universidad por haberme permitido formarme en ella, gracias a todas las personas que fueron participes de este proyecto, ya sea de manera directa o indirecta, gracias a todos ustedes, que fueron los responsables de realizar su pequeño aporte, que el día de hoy se vería reflejados en la culminación de mi paso por la universidad.

A la Tutora María Alicia Suxe Ramírez, por su paciencia y asesoramiento, sin su apoyo yo no habría sido capaz de concluir con éxito este proyecto.
A todos ellos, muchas Gracias.

Pedro Jesús Colonia Hernández

RESUMEN

Esta tesis fue desarrollada bajo la línea de investigación: Implementación de Tecnologías de Información y Comunicación (TIC) para la mejora continua de la calidad en organizaciones en Perú, de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Católica los Ángeles de Chimbote; la problemática es la inseguridad de información, como objetivo realizar la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017, de tal forma minimice la pérdida de información. La investigación fue desarrollada cuantitativamente bajo el diseño descriptivo de transcripción no experimental. La población de la muestra fue constituida por los 30 empleados; de los cuales se obtuvo como resultado: el 73.33% de los empleados encuestados expresaron NO están satisfacción con la seguridad de información actual; mientras el 26.67% indicó que, SI se encuentran satisfacción con la seguridad de información actual, el 100.00% de los empleados encuestados expresaron SI necesidad de la propuesta de un sistema de la información con normas ISO 27001. El alcance abarca un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para preservar la confidencialidad, integridad y disponibilidad de la información en la Municipalidad Distrital de Buena Vista Alta. En conclusión, se determinó que la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta mejoro sus procesos de seguridad de la información y comunicación.

Palabras clave: Confidencialidad de la información, ISO, Integridad de la información, Seguridad, TIC.

ABSTRACT

This thesis was developed under the line of research: Implementation of Information and Communication Technologies (ICT) for the continuous improvement of quality in organizations in Peru, of the Professional School of Systems Engineering of the Catholic University of Los Angeles de Chimbote; The problem is the insecurity of the information, as the objective of the proposal of an information security management system with the ISO 27001 standards for the District Municipality of Buena Vista Alta - Casma; 2017, so minimize the loss of information. The research was developed quantitatively under the descriptive design of non-experimental transcription. The sample population was made up of 30 employees; of which were obtained as a result: 73.33% of the employees surveyed said they are NOT satisfied with the security of the current information; while 26.67% indicated that, IF they found satisfaction with the current information security, 100.00% of the employees surveyed expressed YES the need for the proposal of an information system with ISO 27001 standards. The scope covers a security management system of information based on ISO / IEC 27001 to preserve the confidentiality, integrity and availability of information in the District Municipality of Buena Vista Alta. In conclusion, the proposal for an information security management system was determined with the ISO 27001 standards for the District Municipality of Buena Vista Alta, best of its information and communication security processes.

Keywords: Confidentiality of information, ISO, Integrity of information, Security, ICT.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

I. INTRODUCCIÓN

En las plataformas tecnológicas, actualmente hay mucha vulnerabilidad y amenazas que conducen a la perdida de información siendo este un bien importante para las empresas ya que mediante ellas pueden tomar decisiones adecuadas, las mismas que dependerán de la integridad, confidencialidad y seguridad de los datos que actualmente se encuentran en conflictos por diversas razones de controles empresariales ya que muchas de ellas no cuentan con políticas y normas que regulen el uso de las tecnologías y sistemas de información. Haciendo que exista conflictos de seguridad y confidencialidad. Para que las personas puedan hacer un uso responsable se deben establecer políticas alineadas a la gestión de la seguridad de la Información, en ese sentido la ISO / IEC 27001, contribuye a que las organizaciones cuenten con Sistemas de Gestión de Seguridad de la Información, que ayudara a monitorear la implementación, uso y control de los sistemas de información desde su elaboración hasta su ejecución, velando de manera idónea por las tecnologías de información que lo soporta (1).

La seguridad de la información es una regla asociada tradicionalmente a la gestión de TIC, cuyo propósito es mantener niveles admisibles de riesgo de la información organizacional y de los dispositivos tecnológicos que aprueban su recolección, procesamiento, acceso, intercambio, almacenamiento, transformación y adecuada presentación. La norma ISO/IEC 27001 que permite la garantía, la confidencialidad y la integridad de los datos e información (2).

La Municipalidad Distrital de Buena Vista Alta, es una entidad administrativa que agrupa una sola localidad, como es el caso de la ciudad de Casma. Esta institución se rige principalmente en lo que prescribe la Constitución Política de la Republica y en la Ley de Régimen Municipal en que establece la autonomía funcional, económica y administrativa de la entidad. No cuentan con una Política de Normalización de la seguridad de Información que pueda impedir la pérdida y eliminación de información que le pertenecen a la Municipalidad.

De acuerdo a lo planteado surge la siguiente pregunta: ¿De qué manera la propuesta de un Sistema de Gestión de Seguridad de la Información con Normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017, permitirá minimizar la pérdida de información?

A fin de dar solución a la pregunta formulada se planteó el siguiente objetivo General: Realizar una propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017, de tal forma minimice la pérdida de información.

Para dar cumplimiento al objetivo general, se plantearon los siguientes objetivos específicos:

1. Analizar la seguridad actual de la información, en la Municipalidad Distrital de Buena Vista Alta - Casma.

2. Evaluar los marcos de referencias que ayuden a mejorar la seguridad de la información en la Municipalidad Distrital de Buena Vista Alta - Casma.

3. Proponer la aplicación de la Norma ISO / IEC 27001, para mejorar la seguridad de la información en la Municipalidad Distrital de Buena Vista Alta - Casma.

La presente investigación tiene su justificación académica, teniendo en cuenta el conocimiento adquirido durante todos los años de estudio en la Universidad Católica de Los Ángeles de Chimbote fue utilizado, lo cual nos servirá para realizar la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital Buena Vista Alta.

Asimismo, se justifica operativamente: Se basa en los objetivos específicos de la presente investigación, que permitirá el Municipio Distrital Buena Vista Alta tener una mejor gestión en seguridad de la información, organización de TIC y gestión de activos.

Como Justificación económica: Su finalidad es ahorrar tiempo y dinero, ya que al implementarse estas políticas de seguridad no generan costos excesivos, permitiendo el ahorro a la Municipio Distrital Buena Vista Alta.

Como Justificación tecnológica; En el Municipio Distrital Buena Vista Alta, se diferencia de otros municipios en el mejoramiento de la gestión de las TIC.

Como Justificación institucional; Otorgara la Municipalidad Distrital de Buena Vista Alta, proteger la viabilidad, confiabilidad y seguridad de las informaciones.

El alcance del presente proyecto, abarca un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para preservar la confidencialidad, integridad y disponibilidad de la información en la Municipalidad Distrital de Buena Vista Alta, con la finalidad de que los riesgos sean conocidos y minimizados.

La metodología que se usó en la presente investigación tiene como diseño no experimental de tipo descriptiva y de nivel cuantitativo.

El principal resultado conforma con una cantidad de la muestra que está constituido por 30 empleados; de los cuales se obtuvo como resultado: el 73.33% de los empleados encuestados expresaron NO están satisfacción con la seguridad de información actual; mientras el 26.67% indicó que, SI se encuentran satisfacción con la seguridad de información actual, el 100.00% de los empleados encuestados expresaron SI necesidad de la propuesta de un sistema de la información con normas ISO 27001.

En conclusión, determinó mejorar la seguridad de la información de la Municipalidad Distrital de Buena Vista Alta, para minimizar la pérdida de información y brindar mayor seguridad.

II. REVISIÓN DE LA LITERATURA

2.1. Antecedentes

2.1.1. Antecedentes a nivel internacional

En el año 2015, el autor Guamán J. (3), realizo una tesis titulada "Diseño de un sistema de gestión de seguridad de la información para instituciones militares", que se realizó en la Escuela Politécnica Nacional ubicado en Quito – Ecuador, el presente trabajo de tesis tiene como objetivo principal diseñar un sistema de gestión de seguridad de la información para instituciones militares, que incorpore estándares internacionales y comunicaciones con el fin de contribuir a la modernización de las instituciones militares, la metodología de la investigación fue sustentada por el autor en tres fases fundamentales: la primera el estudio diagnóstico, la segunda la factibilidad y la tercera el diseño de un sistema de gestión de la seguridad de la información para instituciones militares, tomando como referencia la norma ISO 27001:2005 y utilizando una combinación de metodologías para la evaluación de riesgos que ayuda a tomar decisiones sobre las opciones apropiadas de tratamiento de riesgos. En conclusión, es necesario realizar el diseño de un sistema de gestión de seguridad de la información para instituciones militares, que minimicen los riesgos físicos y lógicos de la información que se transmiten, procesa, almacena y distribuye a través del sistema de comunicaciones, para la utilización de los servicios y sistemas por los usuarios de los repartos militares y navales.

Según los autores Bermúdez, K. y C Bailón, E. (4), en la tesis "Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001 – sistemas de gestión de seguridad de la información

dirigido a una empresa de servicios financieros", que se ha realizado en la Universidad Politécnica SALESIANA, ubicado en el país de Ecuador, en el año 2015, el presente trabajo de tesis tiene como objetivo analizar los procesos críticos de Credigestión respecto a las gestiones de seguridad adecuadas para garantizar la confidencialidad, integridad y disponibilidad de la información, mediante la formulación recomendaciones de seguridad y controles basados en la Norma ISO/IEC 27001. La investigación se realizará tomando como referencia una metodología de implementación, tomado en cuenta lo indicado en la norma ISO/IEC 27001 y de acuerdo a la realidad de aplicación dentro de la empresa a la cual se dirigió a la investigación. Cuya población se totaliza en 230 empleados y la muestra se seleccionó a 23 funcionarios. Los resultados obtenidos en la evaluación del análisis de Seguridad de la Información y Seguridad Informática, ayudara a Credigestión en la implementación de buenas prácticas que mitigara las vulnerabilidades y amenazas que han sido identificadas. En conclusión, el análisis realizado demuestra que los activos de información de las áreas consideradas críticas y la situación actual de la empresa con respecto a la seguridad de la información, refleja potenciales índices de riesgos, los cuales exponen a la información de daño, robo o modificaciones que pueden causar un impacto negativo dentro de las actividades del negocio.

Según los autores Yagual, C. y Chilán, L. (5), en la tesis "Análisis para la integración de un Sistema de Gestión de Seguridad de Información (SGSI) ISO-27001 Utilizando OSSIM para empresa Industrial", que se realizó en la Universidad Politécnica SALESIANA, ubicado en el país de Ecuador, en el año 2014, el presente trabajo de tesis tiene como objetivo general minimizar los riesgos de seguridad de la información mediante el análisis previo a la implementación de la norma ISO 27001 combinando
las herramientas de seguridad que ofrece OSSIM logrando así el fortalecimiento de un sistema de gestión de control eficiente para el área

de Tecnología de información, Para este caso de estudio se usó el método de investigación de riesgo llamado “Magerit”,la cual nos guio con la realización de una matriz de evaluación y riesgo para cada proceso de la empresa, determinando que tan expuesto se encontraba un activo hacia alguna vulnerabilidad. En conclusión, se propone un plan de contingencia para el área de TI tratando de prevenir las situaciones las cuales se pudiera presentar un siniestro que signifique una paralización de las operaciones informáticas, con sus consecuentes perdidas.

2.1.2. Antecedentes a nivel nacional

Según el autor Seclén J. (6), en el año 2016, menciona en su tesis titulada "Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001", realizado en la Universidad Nacional Mayor de San Marcos ubicado en la ciudad de Lima - Perú, la investigación tuvo una metodología cualitativa, ya que tiene como objetivo la indagación descriptiva de los factores que afectan la implementación del Sistema de Gestión de Seguridad de la Información en las Entidades de la Administración Pública según la NTP-ISO/IEC 27001, la investigación es inductiva, ya que pretende obtener conclusiones generales a partir de los resultados obtenidos en el levantamiento de información de las entidades públicas.

Talavera V. (7), realizó una investigación titulada “Diseño de un Sistema de Gestión de Seguridad de Información para una Entidad
Estatal de Salud de acuerdo a la ISO/IEC 27001:2013”, se presentó en la Universidad Católica del Perú de Lima, realizado en el año 2015, el presente trabajo de tesis tiene como objetivo principal Diseñar un sistema de gestión de seguridad de la información para una institución estatal de salud, de acuerdo a la norma ISO/IEC 27001:2013.La metodología de investigación fue diseño no experimental de tipo descriptiva, y tener un estudio actual de los principales procesos que

involucra el manejo de información crítica para el INMP – según el alcance establecido para el mismo – así como del establecimiento del análisis y diseño de un SGSI en una organización de este tipo, teniendo en cuenta el cumplimiento de las normas actuales que se apliquen a estos procesos críticos. En el presente proyecto pretende realizar un análisis y diseño que permita la implementación de un SGSI a medida para una institución del sector salud, que a la vez cumpla con las leyes y normas superiores que rigen aspectos similares a los que el presente proyecto pretende dar solución.

Aguirre D. (8), realizó una investigación titulada "Diseño de un Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A.", se presentó en la Universidad Católica de Lima, realizado en el año 2014, el presente trabajo de tesis tiene como objetivo principal Diseñar un sistema de gestión de seguridad de información para SERPOST según lo indicado por la NTP ISO/IEC 27001:2008 y la NTP-ISO/IEC 17999:2007 de seguridad de información. La metodología de investigación fue diseño no experimental de tipo descriptiva, su resultado se logró a través del desarrollo de un "Business Case" buscamos obtener el apoyo de la alta dirección de la entidad pública para poder implementar adecuadamente este sistema de gestión. En conclusión es necesario difundir las normas de seguridad existentes y establecer charlas de capacitación y concientización en toda la empresa, esto debido a la poca cultura de seguridad que existe en la organización, desde las planas gerenciales hasta el personal operativo, incluyendo al personal de seguridad, debido a que se ha detectado que existen controles normados; sin embargo, estos no son conocidos por el personal y no existen métricas que permitan monitorear el cumplimiento de estas normas.

2.1.3. Antecedentes a nivel regional

Según el autor Castillo R. (9), en su tesis de maestría titulada "Sistema de Gestión de Seguridad de la Información en la Municipalidad Distrital de Pira aplicando la norma ISO/IEC 27001:2013"; en el año 2016, realizado en la Universidad Católica Los Ángeles de Chimbote , el presente trabajo de tesis tiene como objetivo principal es evaluar el sistema de gestión de seguridad de la información en la Municipalidad Distrital de Pira basado en la norma ISO/IEC 27001:2013; la cual permitirá una mejor administración en los activos de información. El autor define la metodología de investigación por el grado de cuantificación reúne las condiciones de una investigación cuantitativa, el investigador para la presente investigación, se tomó como población a todo el personal administrativo que consta de 16 trabajadores que labora en la oficina matriz de la Municipalidad Distrital de Pira, que son aquellos involucrados directamente en los procesos, para cada una de las variables en estudio sobre sistemas de gestión de seguridad de la información, al finalizar el proceso de evaluación. Según los resultados de la encuesta aplicada a los trabajadores se determinó que no cuentan con el conocimiento y las medidas adecuadas para salvaguardar los activos de información. Con el Autodiagnóstico General para la evaluación de madurez, el 93% consideran por conocimiento que, en la Municipalidad, este proceso está en el nivel Inexistente, según los niveles de madurez de la ISO/IEC 27001:2013, lo que significa que se reconoce la necesidad de recolectar y evaluar información sobre los procesos de monitoreo. El 7% No se han identificado procesos estándar de recolección y evaluación. En conclusión, esta evaluación permite a la empresa tomar medidas preventivas y correctivas en los procesos que necesitan ser atendidos con mayor brevedad a nivel de seguridad para el mejor funcionamiento de los mismos.

Nizama M. (10) ,en su tesis titulado “Evaluación de la seguridad para el personal informático y usuarios de sistemas en la Municipalidad Provincial de Piura”, se presentó en la Universidad Católica los Ángeles de Chimbote, en el año 2015, el presente trabajo de tesis tiene como objetivo principal determina el nivel de evaluación de la seguridad para el personal informático y usuarios de sistemas, mediante el uso de listas de verificación estandarizadas para una auditoría a la seguridad informática, aplicadas a diversos trabajadores de las diferentes áreas y oficinas de la Municipalidad Provincial de Piura, durante el período octubre-diciembre 2014. La metodología de la investigación fue descriptiva cuantitativa; cuya población en totalidad es de 480 trabajadores que laboraban y la muestra estuvo constituida por 50 trabajadores administrativos. Los resultados que se obtuvieron fueron: respecto a la dimensión de protección contra riesgos y contingencias relacionadas con el ambiente de trabajo más de la mitad de los usuarios 60% no está de acuerdo ni en desacuerdo, en cuanto a la dimensión de protección contra riesgos y contingencias por factores meteorológicos y desastres naturales hay un 3% de usuarios en desacuerdo, y solo un 11% está totalmente de acuerdo, y en la dimensión de protección contra riesgos y contingencias derivados del suministro de energía eléctrica más de la mitad de los usuarios 58% están en desacuerdo. En cuanto a las conclusiones, se puede indicar, en primer lugar, que se registra una relativa seguridad a nivel de protección de su ambiente de trabajo, asimismo, también se registra una relativa seguridad respecto al nivel de protección contra factores meteorológicos, aunque con valores polarizados. También se registra que en general no se confía en que se garantice una continuidad de los servicios de energía eléctrica.

Según el De la Cruz A. (11), en su trabajo de investigación titulado

“Mejora del programa de seguridad basada en el comportamiento del sistema integrado de gestión de prevención de riesgos y medio ambiente de GYM S.A”, se presentó en la Universidad de Piura, en el año 2014, tiene como fin dar a conocer las bases teóricas, conceptuales y técnicas de la Seguridad Basada en el Comportamiento (SBC) orientada a cambiar los comportamientos inseguros de los trabajadores por comportamientos seguros logrando mantenerlos en el tiempo. Además, busca contribuir al Sistema Integrado de Gestión (SIG) de la empresa Graña y Montero (GyM) en la reducción de incidentes, accidentes, lesiones producidas por actos o comportamientos inseguros. Esto implica comprender la estructura y metodología de implementación de un programa de seguridad basada en el comportamiento, y con todo ello proponer mejoras en el programa de SBC de GyM. De ambos sistemas, sistema cliente y sistema GyM, se rescatarán los puntos importantes y ventajosos realizando un análisis FODA; una vez obtenido dichos puntos, se identifican las falencias y faltas del programa de la SBC, logrando así un mejoramiento al programa de seguridad basada en el comportamiento, y finalmente se propondrá el procedimiento de implementación y ejecución de la SBC. En conclusión, de todo ello, se llegará a obtener un formulario GyM, en el que se presenten las conductas y comportamientos de las personas, y se pueda observar si es seguro o si no lo es, identificando las causas inmediatas y causas a raíz de sus comportamientos.

2.2. Bases teóricas

2.2.1 Rubro de la empresa

El municipio del distrito de Buena Vista Alta es una corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio, que corresponde a la administración de una comuna o grupo de comunas, y cuya finalidad es satisfacer las necesidades de la comunidad. Asegurar su participación en el progreso económico social y cultural de la comunidad o grupo de municipios (12).

El Sector Público en Perú

Características

El Perú se denomina una república democrática, soberana e independiente y social, establecido constitucionalmente en el año 1993, la misma que es dirigida por el Congreso. A través del referéndum realizado históricamente en octubre del día 31, en el día señalado se creó la constitución política que establece la autonomía y responsabilidades del presidente de la república, consejos de ministros, poder legislativo, formado por los congresistas elegidos por voto regional (13).

- **Constitución Política del Perú**

La constitución se creó en el año 1992 y se activa a partir del 29 de diciembre de 1992. Su argumento está desarrollado por títulos que son seis, 206 artículos, además con disposiciones teniendo una cantidad de 16 y transitorias (13).

- Administración Financiera Gubernamental

La gestión financiera del estado es administrada por el Ministerio de Economía y Finanzas, el mismo que cuenta con unidades operativas como la Dirección General de Crédito Público, el cual se encarga de equilibrar los costos y presupuestos financieros que se asignan del estado al sector público, salvaguardando el endeudamiento y operaciones que se requieran ejecutar con el tesoro público. La Dirección General de Crédito Público, actúa como agente de entidades de crédito del Estado, pero puede designar a otro agente de entidades de crédito. Los procesos de endeudamiento público interno, directo y/o con aval del gobierno central peruano se aprueban por Decreto Supremo, con el voto del Consejo de Ministros, autorizado por el Ministro de Economía y Finanzas y por el ministro del sector. Las operaciones de endeudamiento externo se aprueban por Decreto Supremo, con el voto aprobatorio del Consejo de Ministros refrendado por el Ministro de Economía y Finanzas y por el ministro del Sector. Las operaciones de endeudamiento externo que no conllevan garantía del gobierno central se aprueban por acuerdo de sus respectivos directorios u órganos equivalentes, previa autorización por Resolución Suprema refrendada por el Ministro de Economía y Finanzas y por el Ministro del Sector. La ley del Sistema Nacional de Control, Decreto Ley 26162 precisa que la Contraloría General de la República tiene autonomía técnica, funcional, administrativa y financiera. Siendo esta una entidad pública descentralizada, la Contraloría tiene acceso en cualquier momento e ilimitación a los registros documentos, e información de las entidades, aun cuando sean secretos (14).

2.2.2 Municipios en el Estado Peruano.

El significado de Municipalidad

Son organizaciones que conforma el estado, personal jurídico para el alcance de mayor ventaja de las gestiones de las Municipalidades distritales o provinciales, haciendo una mejor administración para resolver los problemas y necesidades que los residentes necesitan en su rango demográfico. Los gobiernos o municipios locales son organismos que constituyen la estructura del estado peruano. Cada uno de los municipios distritales tiene ciertas diferencias entre sí, sin embargo, obtiene el mismo nivel con la comunidad, a fin de dar solución a los problemas ciudadanos y apoyando de esta manera a la gobernabilidad del estado Peruano (15).

- Reseña de los Municipios.

Los municipios de Perú se dividen en provincias, distritos y áreas urbanas creadas con las últimas regulaciones municipales y se rigen por regulaciones gubernamentales. Sus características principales incluyen la gestión de tierras y terrenos en su área, de acuerdo con la normativa vigente en materia de protección del medio ambiente, la seguridad pública, velando por el patrimonio histórico y paisajístico de su área, promoviendo el desarrollo económico de su área urbana y promoviendo la participación comunitaria, especialmente en el uso y control de recursos, desarrollar servicios sociales para proteger los bajos ingresos, combatir la comercialización y el consumo de drogas. Controversia entre los representantes de la corona española y los representantes de una doctrina libertaria de mentores intelectuales inspirada en la gran revolución política inspirada en el liberalismo. En Perú, le costó

mucho obtener su libertad y tomar un gobierno democrático, con esta fuerza formó el conjunto de las fuerzas españolas y fue llamado la independencia de la República. El Gobierno Municipal, indicaba una autonomía administrativa que fue su creación en ese momento para la expresión de la sociedad del Perú. En el año 1960, se inició la creación de la economía y administrativa para los municipios, que fueron creadas y aprobadas por las organizaciones en grupo de personas en las localidades y ciudades (16).

Son organismos gubernamentales que, en el Perú, reciben el nombre de Municipalidades, El punto de partida es el ayuntamiento, ejemplos de gobierno local creados bajo el virreinato. Actualmente existen alrededor de 1855 municipios entre el distrito y la provincia. Los Municipios están dentro de la organización territorial del Estado y de los canales inmediatos de participación del barrio en asuntos públicos que son responsables por la gestión autónoma de los intereses de su comunidad; siendo elementos esenciales del gobierno local, territorio, población y organización. La estructura orgánica de los municipios consiste en el ayuntamiento y la oficina del alcalde. Los municipios tienen un carácter de autonomía política, económica y administrativa en materias de su competencia (16).

Tipos de Municipalidades

Municipalidad tenemos:

- Municipalidades Provinciales, tiene la función de coordinar y apoyar los gobiernos de municipios distritales.

- Los municipios distritales, tienen la función de ejercer la gestión local de acuerdo a los procesos establecidos.

- Las Municipalidades de centros poblados, son autorizados y se desarrollan por orden de la Municipalidad provincial a fin de realizar funciones delegadas además con el propósito en la ordenanza que las crea (16).

Determinación Estadístico de Municipalidades

En las Instituciones de Estadística e Informática ha puesto en marcha a las autoridades para la disposición de la sociedad, privadas y públicas en general para la aprobación de Centros Poblados en el año 2017, cuya función es dar un aporte interesante para la consulta permanente (17).

Tabla Nro. 1: Número de municipios, Total de población proyectada 2015.

Departamento	Municipalidades Provinciales	Municipalidades Distritales	Municipalidades de Centros Poblados	Población Total Proyectada al 30/06/2017
Total	**196**	**1 655**	**2 534**	**31 826 018**
Amazonas	7	77	74	424 952
Áncash	20	146	217	1 160 490
Apurímac	7	74	97	462 791
Arequipa	8	101	23	1 315 528
Ayacucho	11	105	159	703 628
Cajamarca	13	114	345	1 537 172
Prov. Const. del Callao	1	6	-	1 042 496
Cusco	13	97	131	1 331 758
Huancavelica	7	90	260	502 084
Huánuco	11	66	260	873 134
Ica	5	38	5	802 610
Junín	9	114	108	1 370 141
La Libertad	12	71	96	1 905 301
Lambayeque	3	35	39	1 280 788
Lima	10	161	57	10 139 213
Loreto	8	45	22	1 058 946
Madre de Dios	3	8	10	143 687
Moquegua	3	17	24	184 187
Pasco	3	26	73	308 723
Piura	8	57	68	1 873 025
Puno	13	96	325	1 442 930
San Martín	10	67	97	862 822
Tacna	4	23	22	350 105
Tumbes	3	10	7	243 362
Ucayali	4	11	15	506 145
Provincia de Lima	1	42	1	9 174 855
Región Lima 1/	9	119	56	964 358

Fuente: INEI – Directorio Nacional de Municipalidades (17).

2.2.3 La Municipalidad Distrital de Buena Vista Alta

- **Información general**

La Municipalidad Distrital de Buenavista Alta, en el gobierno local se conjugo con el personal jurídico de derecho público, con política, en la administrativa para la competencia, ingresando la normatividad determinadas en el marco de la constitución Política del Perú y reglamento de Municipalidades. El distrito de Buenavista Alta es uno de los cuatro distritos de la provincia de Casma, ubicado en el departamento de Ancash, bajo el gobierno administrativo regional de Ancash (12).

Sus limitaciones son:

Norte Santa, Sur Yaután, Este Yungay, Oeste Casma.

División geográfica del Distrito:

Buena Vista Alta, Buena Vista Baja, Cahuacucho, Cunca, Empedrada, Fundo Bejar, Heroes del Cenepa, Hornopampa, Huancamuña, Huanchuy, La Viña, Mojòn Olivar Alto, Olivar Bajo, Paredon, Poyor Alto, Poyor Bajo, Rinconada, Rumipallana, Sechin Alto, Unto, Tucushuanca, Yanacaca Chico, Yanacaca Grande.

Población

Buena Vista Alta tiene una población de 3.937 habitantes de acuerdo con datos del Instituto Nacional de Estadística e Informática del año 2017. De los 3.937 habitantes de Buena Vista Alta, 1.849 son mujeres y 2.088 son hombres.

Por lo tanto, el %53,04 de la población son hombres y el %46,96 mujeres. Si comparamos los datos de Buena Vista Alta con los del departamento de Ancash concluimos que ocupa el puesto 47 de los 166 distritos que hay en el departamento y representa un 0,3702 % de la población total de ésta. A nivel nacional, Buena Vista Alta ocupa el puesto 981 de los 1.833 distritos que hay en Perú y representa un 0,0144 % de la población total del país (17).

Tabla Nro. 2: Resumen de Buena Vista Alta.

Dato	**Valor**
Población total	3.937
Hombres	2.088

Mujeres	1.849
% hombres	53,04
% mujeres	46,96
ranking provincial	47 / 166
ranking nacional	981 / 1.833
Fuente: INEI	**Censo Nacional del 2017**

Fuente: Municipalidad Distrital de Buena Vista Alta (12).

Gráfico Nro. 1: Mapa del Distrito de Buena Vista Alta.

Fuente: Perú top tours (18).

Historia

El Distrito de Buenavista Alta fue creado el 5 de abril de 1935.por la ley 8075 en el Gobierno del presidente Oscar Raimundo Benavides Larrea fue un militar y político peruano Tiene como patrona a la Virgen del Rosario y el segundo domingo de noviembre de cada año se celebra su fiesta patronal, Está conformada por 24 centros Poblados. Los cuáles

se dedican en su gran mayoría a la agricultura, teniendo como principal actividad económica la producción y exportación. Las exportaciones generalmente son mango, palto, uva, maracuyá, y sus centros arqueológicos más visitados son los jeroglíficos de la pampa colorada y la piedra labrada, y casi todos sus caseríos pertenecen a tiempos muy remotos, hablamos desde tiempos prehispanos, cuando los primeros humanos primitivos habitaron en el valle de Sechin y se quedaron miles de años hasta alcanzar su desarrollo cultural (19).

Los pueblos antiguos, incluso en la corteza terrestre, ruinas ocultas que aún están por descubrir por la geología que para ellos es un desafío establecer conclusiones históricas y culturales, está llena de costumbres, tradiciones y leyendas de su pasado histórico, muy acomodadas. Una de sus características importantes es que forma parte de un valle fértil y hermoso (19).

- **Objetivos organizacionales**

  Objetivo estratégico sectorial:

  Proceso Urbano y Medio Ambiente.

  Comprenden los programas y proyectos que impliquen el uso racional de los recursos naturales y de mejoramiento ambiental. Establece y mejora las condiciones de infraestructura básica en armonía con un crecimiento urbano ordenado priorizando la integración vial y aspiración de la población a vivir en un ambiente saludable, permitiendo a Buena Vista Alta convertirse en un distrito sostenible y saludable que respete y consolide la identidad de la ciudad (12).

  Los Procesos Institucionales y sus Capacidades

Incluye programas y proyectos orientados al desarrollo de la comunidad local y la capacidad de los actores organizacionales para fortalecer la capacidad institucional, técnica y de organización municipal para lograr una gestión eficiente, la consolidación del servicio gubernamental en Buena Vista Alta, el apoyo de las instituciones con mayor participación de los ciudadanos en la toma de decisiones. Las distintas unidades en la administración municipal deben cumplir sus compromisos con transparencia, honestidad y eficiencia, citando las estructuras organizativas adecuadas y los instrumentos normativos que las regulan. Así, los gobernantes intentan desde este espacio establecer un buen gobierno donde sea necesario modernizar las viejas formas municipales, guiarlo para hacer Transparencia, Fiable y Eficaz (12).

Objetivos Institucionales Informáticos:

Utilizar de forma eficiente las informaciones y las nuevas Tecnologías de Información y Comunicación (TIC) como recursos para prestar servicios de calidad, accesibles, seguros y oportunos a la Institución, en aplicación de las directrices y normas emitidas por la Oficina Nacional. de Gobierno Electrónico y Computación, órgano regulador del Sistema Nacional de Computación (12).

Objetivos Informáticos Específicos:

- Planificar el diseño de los sistemas informáticos y organizar la infraestructura tecnológica que soporta los procesos de información y comunicación de la Municipalidad, mediante la dirección, supervisión, ejecución y evaluación (12).

- Establecer el marco normativo para la adecuada utilización de los equipos informáticos, definiendo perfil y niveles que permitan acceder de manera segura y confiable a fin de establecer los protocolos de seguridad y calidad en los sistemas informáticos y redes de comunicación (12).

- Establecer el plan anual de desarrollo que permita la articulación de proyección de innovación y tecnologías, los cuales deben estar basados en torno al giro de negocio y las necesidades institucionales del municipio (12).
- Realizar la programación de la implementación, el monitoreo y la evaluación de las actividades asociadas con el soporte técnico a través de la mesa de ayuda que contribuye a las medidas correctivas y preventivas. (12).

Misión

Dar un buen servicio público y el correcto funcionamiento de las actividades organizadas para el bienestar de la comunidad, así mismo contribuir en el liderazgo de la gestión municipal (12).

Visión

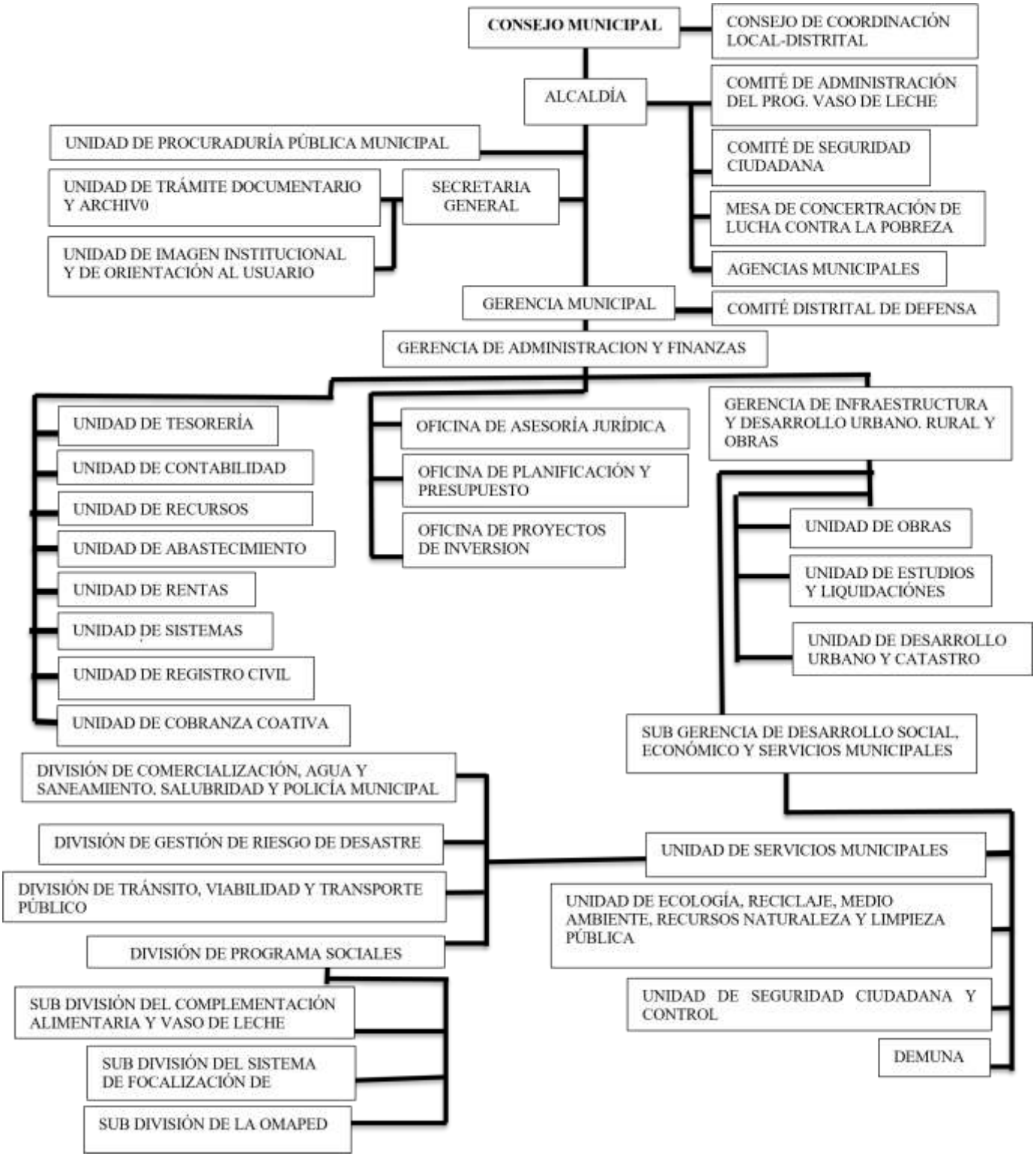
El Distrito de Buena vista Alta, esta con un estado ordenado, limpio, seguro, moderno, integrado y productivo; conjuntamente con importantes servicios en la educación y el seguro de calidad. Buenavista Distrito que fundamentan la persona con valores, identidad y conciencia ciudadana. Accede al gobierno local Distrital democrático, además tiene el rol de ser participativo y transparente (12).

Funciones

La Municipalidad Distrital de Buena Vista Alta, en alcanzar el desarrollar humano, además lo productivo y urbano para los servicios a la comunidad, cuidado del medio ambiente; con un desarrollo económico a nivel local y también los servicios comunitarios, teniendo en cuenta los avances de la inversión pública, privada con método y oportunidades que dan a la cooperación técnica internacional, dando un trabajo estructurado de las políticas nacionales y regionales que tiene para impulsar en ejecutar proyectos y programas para dar un mejoramiento en la sociedad de Buena Vista Alta (12).

- **Organigrama**

Gráfico Nro. 2: Organigrama de la Municipalidad Distrital Provincial de Buenavista Alta.



Fuente: Municipalidad Distrital de Buena Vista Alta (12).

- **Infraestructura tecnológica existente de la Municipalidad Distrital**

Entender que NO es un inventario.

Una tabla para Hardware.

Una tabla para software (SO /Antivirus / etc).

Una tabla para aplicaciones propias de la empresa.

Equipos de Hardware.

Tabla Nro. 3: Hardware.

	CARGO MUNICIPAL	PC	IMPRESORA NORMAL	IMPRESO MATRICIAL	LAPTOP
AMBIENTES PRIMER PISO	GERENCIA DE INFRAESTRUCTURA Y DESARROLLO URBANO RURAL Y OBRAS	2	2		
	OFICINA DE UNIDAD FORMULADORA(UF)	1	1		
	OFICINA DE OPI-ATM.	1	1		
	OFICINA DE TESORERIA	1	1		
	OFICINA DE CONTABILIDAD	1			
	OFICINA DE PLANIFICACION Y PRESUPUESTO	1	1		
	OFICINA DE LA UNIDAD DE SEGURIDAD CIUDADANA	1	1		
	OFICINA-DIV.TRANSITO-VIABILIDAD Y TRANSPORTE PUBLICO		1		1
	OFICINA DE REGISTRO CIVIL	1	1		
	OFICINA DE LA GERENCIA MUNICIPAL	1			
	OFICINA DE LA SECRETARIA GENERAL	1	1		
	OFICINA DEL PROGRAMA DESARROLLO SOCIALVASO DE LECHE	1	1		
	OFICINA DE SERVICIOS COMUNALES Y RENTA	2	1	1	
	OFICINA DE LA DEMUNA	1	1		
	OFICINA DEL JEFE DE IMAGEN	1	1		
	OFICINA DE RECURSOS HUMANOS-LOGISTICA	1	1		
	COMPUTADORAS INTEL CORE I3	17	15	1	1

Fuente: Inventario Tecnológico de la Municipalidad (12).

De acuerdo a la información recopilada de la Municipalidad Distrital de Buenavista Alta tienen ordenadores que son compatible con software para el uso de su trabajo.

Tabla Nro. 4: Sistemas Operativos de la Municipalidad de Buena Vista Alta.

Uso del Sistema Operativo	**Software de Trabajo**
Windows 7	- Programas Ofimática: *Microsoft Office 2016. *Microsoft Excel. - AutoCAD Civil Profesional. - kaspersky antivirus. - Software Utilitario.

Fuente: Inventario Tecnológico de la Municipalidad (12).

2.2.4 Las Tecnologías de información y comunicaciones (TIC)

Sección en TI del Municipio de Buenavista Alta

El departamento de TI, tiene la función de afrontar adecuadamente los servicios, cuenta con unidades operativas especializadas como Coordinación de Informática y de Soporte tecnológico, las cuales se encargan de velar por la correcta atención de los requerimientos y proyectos de gestión para la sociedad (12).

Historia

Desde la década de 1980, el uso de la computadora personal comienza a ser común, lo que parece referirse a la información almacenados. Durante el período de 1990, comenzaron a surgir virus y gusanos y la gente se dio cuenta del peligro que nos acecha como usuarios de PC y computadoras conectadas a Internet. Además de propagar ataques en los sistemas informáticos, y los piratas informáticos de la palabra también se muestran en la prensa. A finales de los 90, la amenaza comenzó a generalizarse, aparecieron nuevos gusanos y un código malicioso generalizado. Y desde el año 2000, los eventos se vieron obligados a tomar la seguridad de los datos muy en serio (20).

Las TIC en el Municipio Distrital de Buenavista Alta

El avance actual de las TIC, han generado nuevas expectativas y cada día soportan procesos más complejos con el fin de atender la globalización y economía. La evolución de la tecnología, para tener nuevas expectativas y muy complejas, usando las mismas formas para la globalización economía que hoy en día, las TIC ofrecen mucho beneficio en la parte competitiva. Con la utilidad de las TIC es una importante mejora en las instituciones centrales, pues automatizan los procesos operativos y alcanzan ventajas competitivas que gestionan la relación de sus rivales (12).

En estos aplicativos principales, posee:

Sistema Integrado de Administración Financiera (SIAF-SP)

El Ministerio de finanzas y economía, con el desamen del Sistema de Ejecución, generaliza la formulación referencial en el marco

presupuestal. Con el mecanismo muy utilizada en el proceso de gestión financiera que obtiene un monto presupuestal generalmente denominadas unidades ejecutoras que conforma un organismo en dos partes como el registro administrativo y además el registro administrativo (21).

Sistema Integrado de Gestión Administrativa

Este sistema informático tiene como función en el ordenamiento y determinar procesos administrativos que conforman a marco de las normas teniendo en cuenta la capacidad establecida por los Sistemas Administrativos del Estado conformando la eficaz, teniendo acceso al manejo ordenado en los procesos, además realiza los procesos administrativos, previo al registro que tienen información de calidad y determinar la información de costos (22).

Sistema de Gestión Documentaria

Esto permite el control de todas las zonas de ubicación física y el estado actual teniendo las capas generado dentro de ellas, además realiza registro y seguimiento con el objetico de integrar apoyo administrativo en soporte con la finalidad en la búsqueda de un expediente rápidamente en el trámite o en el proceso unido y almacenado primero (22).

Sistema de Gestión Tributaria Municipal – SGTM

Es un diseño que es la pieza central para el Área de Administración de las Instituciones Municipales; además tiene las herramientas específicas que permiten automatizar el registro de los contribuyentes para conocer su historial; y permitiendo la determinación en la municipalidad como tributos de Impuestos de impuesto predial,

vehicular, arbitrios municipales, tasas y derechos como las infracciones de tránsito e infracciones administrativas (23).

Portal Web Municipalidad Buenavista Alta.gob.pe

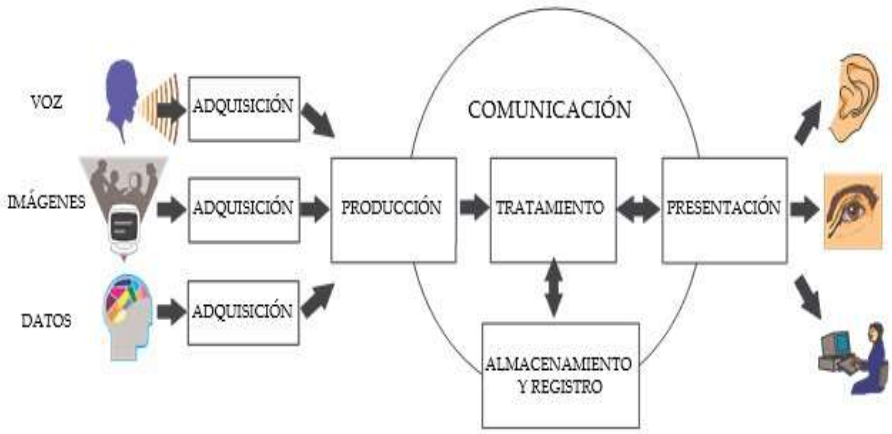
De acuerdo con la normativa vigente, el municipio de distrito Buenavista Alta no tiene realizado un diseñado y administrado por el central portal de transparencia y la aproximación a la información.

2.2.5 Teoría relacionada con la Tecnología de la investigación

Tecnología de la Información

La Tecnología de Información es conjunto de instrumentos para la tecnología que accede a la adquisición, fabricación, almacenamiento, procesamiento, exploración y finalmente para los procesos de información que contiene único propósito de señalización acústica, óptica o electromagnética (24).

Gráfico Nro. 3: El Proceso de la Información.



Fuente: TI, Un enfoque interdisciplinario (25).

Evolución de las TIC

Comenzando en los años 70, donde se empezó a desarrollar la era de la digitalización se hizo con los progresos científicos para la electrónica era importante combinar principalmente electrónicos y software, pero también en los años 80, desarrolló una autorización de la electrónica, además con las telecomunicaciones y también las interconexiones entre redes. El cambio evolutivo de la TIC comenzó con el beneficio para la economía nueva que tenga que ver con criterios de éxito en las organizaciones o incluso la sociedad para entrar en las innovaciones tecnológicas y dar una capacidad para aprender a explotarlos para su propio beneficio, ha facilitado esta tecnología están en la preparación de documentos, enviar y recibir correo electrónico y otras funciones importantes. El punto de similitud entre la revolución de la tecnología es verdaderamente en la revolución industrial, que fue la mayor diferencia en materia prima, es decir, la explosión social basada en la utilización de empresas de energía. Incluidos las áreas, está ciencias como microelectrónica, computación, telecomunicaciones e ingeniería genética (26).

Gráfico Nro. 4: Origen y Evolución de la TIC.

Fuente: Sutori (27).

Áreas de herramientas de Aplicación de las TIC

La agenda digital peruana, dijo que el gobierno peruano se enfrenta al desafío de promover el trabajo del gobierno donde la situación tiene una mayor población, además obtiene un bajo nivel socioeconómico que verifica una gama de propuestas en servicios en instituciones bancarias limitadas para realizar un nivel de alfabetización digital en ocasiones especiales en áreas rurales y remotas, con el cálculo preciso ilimitado para tener un que proponer en las TIC por reconociendo en entidades generales y a su vez obtiene un sistema de información, además con la integración en sus sistemas informáticos, que procede a la última integración en áreas de electrónica entre agencias en él estado. Para detener las reglas de orden necesarias y los procedimientos para la administración pública aceptar e incentivar procedimientos electrónicos en su operación diaria la aplicación de las TIC en la administración pública ha sido intensa en algunas de sus entidades, resultando en islas de modernidad cuyo desarrollo tecnológico establece una gran diferencia con el nivel medio de desarrollo de otras entidades públicas
(28).

2.2.5.1 Las Normas Técnicas Peruanas

> Son documentos de aplicación voluntaria, adoptados por la Comisión de Reglamentos Técnicos y Comerciales - CNB Indecopi y desarrollados por los Comités Técnicos de Normalización, que están compuestos por representantes de los sectores implicados en una actividad definida bajo la supervisión del Indecopi elaboran proyectos de NTP relacionados con su rama actividad, y participar: productor / exportador, sector técnico y consumido (29).

Seguridad de Información

La protección tiene como finalidad la integridad y disponibilidad de los medios de información, para tener un seguro muy efectivo que sea accesible sólo a las personas aceptables, para que ello exija cambios no deseados y que los usuarios sean accedidos cuando precisen (30).

La Organización Internacional de Normalización (ISO) define la seguridad de la información (SI) como:

La preservación de la privacidad, integridad y disponibilidad de información; así como los sistemas involucrados en su tratamiento dentro de una organización. Además, otras propiedades también pueden estar involucradas, tales como: autenticidad, responsabilidad, no repudio y confiabilidad (30).

- Es decir, estos tres términos constituyen la base de la seguridad de la información, de la que se resume la explicación a continuación.

- Privacidad: la información no está disponible o revela individuos, dispositivos o procesos no autorizados.

- Mantenga la exactitud y la integridad de la información y sus métodos de proceso.

- Integridad: Mantener la integridad y precisión de la información y sus procedimientos. Para garantizar la integridad de la información, el remitente siempre debe

autenticarse. Esto puede ser afectado por hardware o productos de virus de malware.

- Acceso: entrada y uso de un sistema de información por parte de las mismas personas, entidades o procesos permitidos cuando lo requieran.

Sistema de Gestión de Seguridad de Información

SGSI tiene capacidad de crear, realizar, manejar, monitorear y mejora la protección de la información que busca para poder identificar el mismo contenido con integridad y disponibilidad, integridad y descarte en la información, minimizando los riesgos de seguridad del ordenador (31).

Gráfico Nro. 5: Ciclo Deming o circulo PDCA.

Fuente: SQL Consultores (32).

Análisis y Evaluación de Riesgo

El análisis de riesgos como la elección de los mecanismos de protección, permite estimar la posible pérdida de información y ayuda a reducirla al facilitar su elección. El método para analizar y gestionar los riesgos del sistema de información es el núcleo de las medidas de análisis, evaluación y gestión de riesgos. Esta metodología analiza los riesgos, identifica las amenazas y su impacto y gestiona el riesgo en base a: Elementos, Eventos, Procesos (33).

En 2008, se definieron tres riesgos, como los riesgos estratégicos asociados con la seguridad de la información, que se centran más en los beneficios y la reputación de la organización, teniendo en cuenta la decisión estratégica tomada por la corporación. Las contingencias tácticas generalmente están vinculados a los sistemas que monitorean la identificación de la manipulación y monitoreo de las contingencias de la información (34).

2.2.5.2 Amenazas

Según la norma ISO 27000, la causa potencial de un suceso no deseado se considera una amenaza, que puede causar daños a un sistema una organización. Alexander y otros (35), coinciden en que las amenazas pueden ser clasificadas en grandes grupos para facilitar la toma de decisiones genéricas que reducen grupos de amenazas durante una acción. Los grupos propuestos son:

- Naturaleza: fenómenos naturales o desastres naturales.

- Humanas Accidentales: Falta de conocimiento, negligencia, terminación, pérdida accidental de los dotas.

- Humanas Intencionales: Amenazas y ataques de información.

- Tecnológico: virus, hackers, crackers, pérdida de datos, software, hardware o errores de red.

Una vez que se han identificado todas las amenazas, se evalúa su potencial de ocurrencia. El resultado de esta evaluación identificará las amenazas de la competencia más alta a la más baja y la decisión de atacar y qué desechar de acuerdo con los criterios, legal y rentable (35).

2.2.5.3 Vulnerabilidades

Las amenazas y las vulnerabilidades están interrelacionadas, forma parte de la pregunta sobre qué vulnerabilidades son explotadas por amenazas, la generación de una inseguridad identificada crea amenazas expuestas a un sistema de información. Esto es lo que para los expertos en cuestiones de seguridad de la información se conoce como la relación de causa y efecto entre los elementos del análisis de riesgo. Por lo tanto, el siguiente paso será integrar estos elementos para analizar y definir los niveles de riesgo que permitirán implementar los procedimientos que ayudarán a mitigar estos riesgos y eliminar las vulnerabilidades (36).

2.2.5.4 Cálculo de Riesgo

Después de que los activos se enumeran y se clasifican y las amenazas y vulnerabilidades se identifican, se calcula el riesgo.

Este cálculo utilizará valores cuantitativos porque el valor de un activo de información se evalúa en el impacto sobre las pérdidas económicas que genera si es violado (36). otros, el análisis de riesgo puede realizarse de dos formas:

- Análisis cuantitativo. Con base en los valores de métricas y calculando que determinan el cálculo de costo-beneficio Requiere mucho esfuerzo, pero permite la comparación de valores.

- Análisis cualitativo ¿Es más flexible, pero el resultado es más subjetivo, no está basado? En número y contiene análisis simples. No permiten la comparación de valores más allá de la disposición relativa.

2.2.5.5 Tratamiento de Riesgos

A partir del informe de evaluación de riesgos se procede a examinar cual es el tratamiento más adecuado para cada uno de los riesgos que han sido identificados (36).

Los siguientes lineamientos de la norma ISO 27001:2005, el procedimiento de riesgos incluye los siguientes enfoques:

Determinar si el riesgo es aceptable o si requiere un tratamiento, en el caso de que una de las siguientes alternativas se identifique para reducir el riesgo a un nivel aceptable, implantando algún control, Aceptar el riesgo porque no es posible realizar un tratamiento o porque éste resulta demasiado costoso, evitar el riesgo, o transferir el riesgo a una tercera parte (36).

Si se decide mitigar el riesgo, se debe definido que los controles del SGSI deben ser implementados. Además, si se considera necesario se pueden seleccionar controles específicos adicionales (36).

Para definir los controles que se realizarán según el análisis de riesgo, se deben realizar los siguientes pasos:

- Prepare un Documento de Declaración de Aplicabilidad (DDA) donde la lista de controles que se va a implementar es detallada.

- Determine el nivel de inseguridad que es accesible para la empresa.

- Obtenga la aprobación de la dirección de la DDA y los riesgos que no están cubiertos.

- Formular un plan de tratamiento de riesgos cuando sea necesario para reducir los riesgos a un nivel aceptable y realizar los controles considerados necesarios de acuerdo con los requisitos de las acciones de ISO / IEC 27001: 2005 en 4.2.1. f, g y h.

- Preparar los procedimientos con la necesidad de realizar controles.

Control

Los controles se enfocan en manejar el riesgo y además incluyendo políticas, estructuras organizacionales (30).
En estas se clasificaciones en:

- Preventivos: Reducir las vulnerabilidades.

- Detectivos: Detectan amenazas o escenarios antes de permitir que se activen otros controles.
- Correctivos: contrarrestar el efecto del acontecimiento de un riesgo.

- Persuasivos: reducir el riesgo o amenazas.

2.2.5.6 ISO/IEC

La Organización Internacional de Normalización (ISO) define el SGSI como un enfoque sistemático para gestionar la información confidencial en la empresa, para garantizar su seguridad. Abarca personas, procesos y sistemas de TI a través de la aplicación de un proceso de gestión de riesgos. Puede ayudar a pequeñas, medianas y grandes empresas en todas las industrias a mantener la información segura (37).

2.2.5.7 Tipos de Serie de Normas ISO/IEC 27000

- ISO / IEC 27000: es una familia de estándares destinados a ayudar a las organizaciones a mantener sus tareas seguras. Su aplicación hace posible manejar la seguridad de los activos, como información financiera, propiedad intelectual, detalles de empleados o información de terceros (37).

- ISO/IEC 27001: ISO / IEC 27001: es un marco internacional reconocido para las mejores prácticas para un sistema de gestión de seguridad de la información. Le ayuda a identificar los riesgos con su información importante e inserta controles apropiados para ayudarlo a reducir el riesgo.

- ISO/IEC 27002: ISO / IEC 27001: es un marco internacional reconocido para las mejores prácticas para un sistema de gestión de seguridad de la información. Le ayuda a identificar los riesgos con su información importante e inserta controles apropiados para ayudarlo a reducir el riesgo.

- ISO / IEC 27003: determinado en una guía para la implementación del SGSI e información sobre el uso del modelo PDCA y los requisitos de sus diferentes fases.

- ISO / IEC 27004: esta norma específica cómo medir el sistema de medición, qué parámetros medir, cuándo y cómo medirlos. Además, ayuda a las empresas a determinar los objetivos relacionados con los criterios de rendimiento y éxito.

- ISO / IEC 27005: la norma internacional que trata la gestión de riesgos de seguridad de la información. La norma proporciona pautas para gestionar los riesgos de seguridad de la información en una empresa, en particular para cumplir con los requisitos del sistema de gestión de seguridad de la información tal como se define en la norma ISO 27001.

- ISO / IEC 27006: esta norma se complementa con ISO / IEC 17021 y proporciona los requisitos de certificación necesarios para una organización que certifica SGSI de acuerdo con ISO / IEC 27001.

- ISO / IEC 27007: es el estándar más conocido en la familia que requiere un sistema de gestión de seguridad de la

información (SGSI). Es una norma internacional para la cual una organización puede ser certificada, incluso si la certificación es voluntaria.

- ISO / CEI TR 27008: proporciona orientación sobre la auditoría de la implementación y operación de los controles, incluida la verificación del cumplimiento técnico de los controles del sistema de información, de acuerdo con las normas de seguridad establecidas por una organización.

- ISO / IEC 27010: esta norma proporciona controles y directrices que están específicamente relacionados con el inicio, la implementación, el mantenimiento y la mejora de la seguridad de la información en las comunicaciones entre organizaciones y sectores.

- ISO / IEC 27011: Consiste en una guía de administración de seguridad de la información específica para las telecomunicaciones.

- ISO / IEC 27013: se enfoca solo en la implementación integrada de un SGSI según ISO / IEC 27001 y un sistema de gestión de servicios (SMS) ISO / IEC 20000-1.

- ISO / IEC 27014: proporciona orientación sobre conceptos y principios para controlar la seguridad de la información a través de los cuales las organizaciones pueden evaluar, monitorear y comunicar directamente las actividades de seguridad de la información dentro de la organización.

- ISO / IEC TR 27015: proporciona una guía de seguridad para la información adicional y las disposiciones de seguridad de ISO / IEC 27002: 2005 Información para iniciar, implementar, mantener y mejorar la seguridad de la información en organizaciones que brindan servicios financieros.
- ISO/IEC TR 27016: Proporciona orientación sobre cómo una organización puede tomar decisiones para proteger la información y comprender las consecuencias financieras de estas decisiones en relación con los requisitos de recursos en competencia.

- ISO / IEC 27799: 2008: proporciona pautas para los estándares de seguridad de la información para la organización y los métodos de gestión de la seguridad de la información, incluida la selección, implementación y gestión de controles, teniendo en cuenta el entorno de riesgo para la seguridad de la información de la organización.

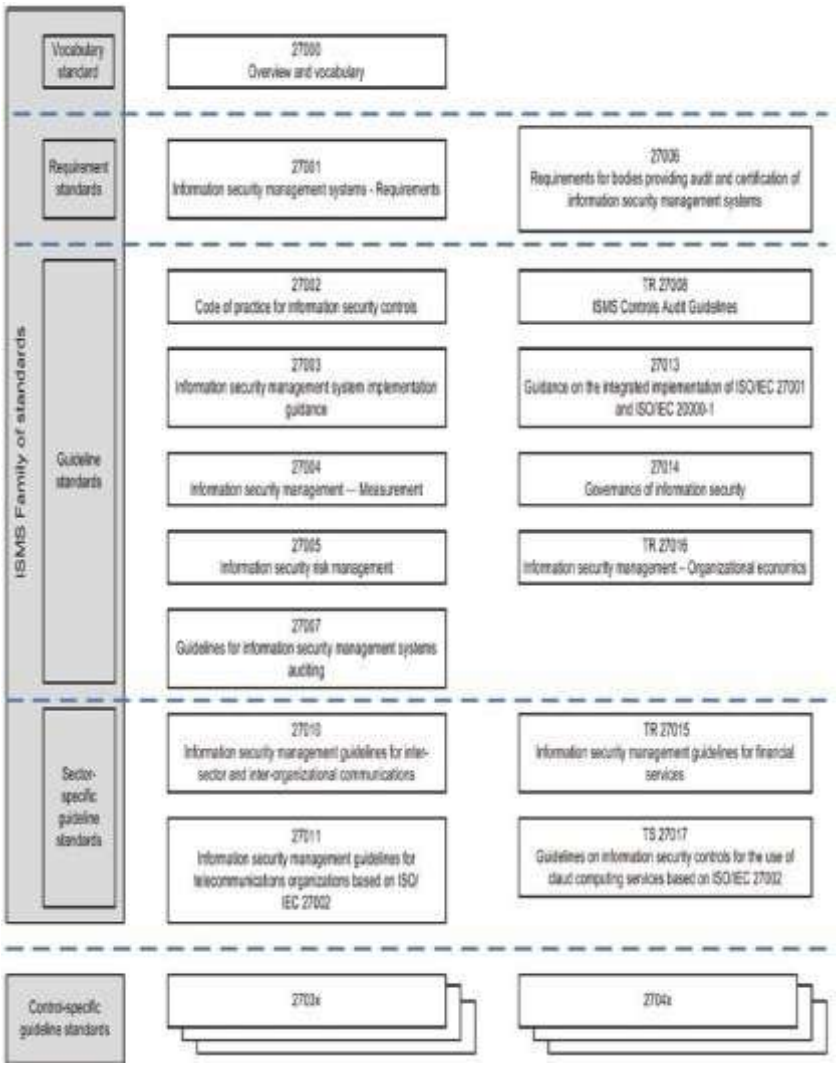
2.2.5.8 Beneficios de ISO 27001

Para 27001 Academy especialistas en brindar asesoramiento mencionan 4 ventajas comerciales fundamentales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información:

- Cumplir con los requerimientos legales.
- Obtener una ventaja comercial.
- Menores costos.
- Una mejor organización.

La seguridad de la información es parte de la gestión global del riesgo en una empresa (37), en el siguiente grafico observamos que áreas interviene:

Gráfico Nro. 6: Relaciones de la familia de estándares ISMS.



Fuente: ISO/IEC 27000:2014 (31)**.**

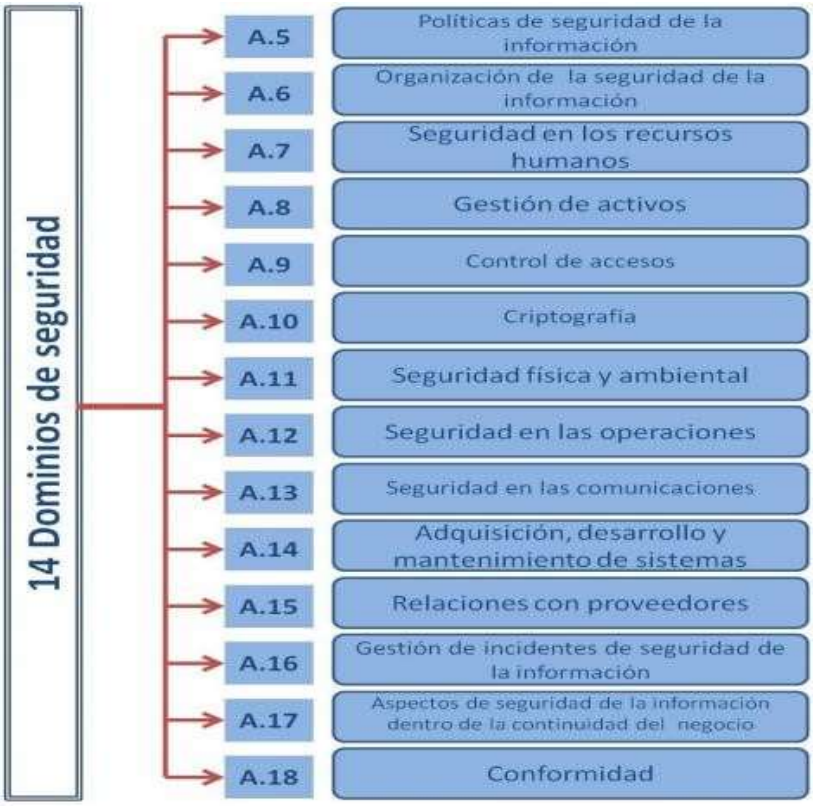
2.2.5.9 Ley de información de gestión de datos técnicos 27001 y su uso Obligatorio

La Ley Técnica Peruana reemplaza a la norma ISO 27001:2008 verificada en el año 2013 como después a sumiría la norma ISO 27001:2013 y además la ISO 27001:2013/COR (38).

El uso obligatorio de la norma ISO 27001:2014 ha sido aprobado en la fecha 14 de enero del 2016. Técnicos de Seguridad, Tecnologías de la Información y el 14 de enero de 2016, se aprobó el uso obligatorio de la ISO 27001: 2014.

Tecnologías de información, técnicos de seguridad, sistema de gestión de seguridad de la información (39).

Gráfico Nro. 7: El nuevo enfoque de la ISO/IEC 27001: 2013.



Fuente: ISACA MADRID CHAPTER (40).

Ventajas del ISMS

Las SGSI son importantes para permitir que tener un plan de negocios destinado a controlar el control de las dificultades en las acciones de negocios y también preservar los métodos graves de Todas las empresas asociadas a fallas importantes en sistemas de formación de desastres (40).

Casos del éxito

En 2014 llevó a cabo la investigación sobre "Análisis de la norma ISO / IEC 27001 en el diseño e implementación de la red

corporativa" de la Universidad Católica de Santiago de Guayaquil, que tiene una seguridad en la aplicación del análisis de la norma ISO / IEC 27001 equipos tener una formación en una empresa o una organización. En el estudio de seguridad de datos, la caracterización general de la Ley ISO 27000 se lleva a cabo para desarrollar a fondo ISO 27001, que es responsable de las tecnologías de seguridad, en última instancia, los requisitos importantes. El plan de seguridad de TI de la compañía está en análisis de riesgo. Este estudio se basa en determinar si la seguridad de la empresa cumple con los parámetros establecidos, lo que permite la mejora y la obtención de la certificación (41).

III. HIPÓTESIS

3.1. Hipótesis General

La propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001, permite minimizar la pérdida de información de la Municipalidad Distrital de Buena Vista Alta – Casma; 2017.

3.2. Hipótesis específicas

1. El análisis de seguridad de la información permite conocer la situación actual de la Municipalidad Distrital de Buena Vista Alta.

2. La evaluación de los marcos de referencia permite una mejor seguridad de la información en la Municipalidad Distrital de Buena Vista.

3. La Propuesta de la aplicación de la Norma ISO/IEC 27001, asegura con seguridad de la información en la Municipalidad Distrital de Buena Vista Alta.

IV. METODOLOGÍA

4.1. Tipo y nivel de la investigación

Por las características de la investigación fue de un enfoque cuantitativo. Asimismo, el tipo de la investigación es descriptiva.

Según Namakforoosh M. (42), la investigación descriptiva busca observar y describir el comportamiento del sujeto de estudio sin influir sobre él de modo alguno. Su objetivo es calcular la proporción de gente de una población específica que posee ciertas características. Una investigación descriptiva es simple cuando se considera una variable.

Según Daniel C. (43) ,la Investigación Cuantitativa, en cambio, es aquella que utiliza preferentemente información cuantitativa o cuantificable. Algunos ejemplos de investigaciones cuantitativas son: diseños experimentales, diseños cuasi – experimentales, investigaciones basadas en la encuesta social.

4.2. Diseño de la investigación

EL diseño de la investigación es no experimental y por la característica de la su ejecución será de corte transversal.

Hernández R., Fernández C. y Baptista P. (44), afirmaron que la investigación no experimental es la investigación que se realiza sin manipular intencionalmente las variables a fin de ver el efecto que pueden producir en otras variables. En la investigación no experimental solo se observa un fenómeno para su posterior análisis. La presente investigación cumple esta característica, debido a que no hay manipulación alguna de la variable, y tampoco se busca hacer algún cambio al fenómeno estudiado durante la investigación.

Es corte transversal porque se analizan las variables en un periodo de tiempo determinado, según en una edición de investigación de la Universidad de Michigan (45), el corte Trasversal ya que el estudio se circunscribe a un momento puntual, recolectando dato en un tiempo único, describiendo variables y analizando su incidencia.

4.3. Población y Muestra

Población

Para la presente investigación la población se delimito a 30 trabajadores en ello tenemos al Gerentes, Subgerentes, Empleados Nombrados bajo el Dec. Leg.276, Bajo el Régimen C.A.S, Bajo el Régimen S.N.P. que pertenecen a

las municipales que utilizan las tecnologías y los sistemas de información de la Municipalidad de Buena Vista Alta.

Según Gómez M. (46) la población es el conjunto total de objetos de estudio.

Muestra

Para la presente investigación, la muestra se seleccionó a 30 trabajadores de la Municipal Distrital de Buena Vista Alta, no se utilizó ninguna técnica estadística, seleccionándolos por conveniencia por ser los involucrados directos en la seguridad de información.

Hernández R, Fernández C y Baptista P. (44), definieron a la muestra como un subgrupo de la población. Un subconjunto de elementos dentro de un conjunto que posee características similares, a la cual se le considera la población. Adicionalmente, estos autores mencionaron que cuando en el caso se incluye todos los elementos del universo o población, se le denomina censo.

Tabla Nro. 5 Resumen de Población.

AREAS DE LA MUNICIPALIDAD	**Nº DE PERSONAS**
Unidad de Estadística e Informática	2
Unidad de Recursos Humanos	2
Unidad de Logística	3
Unidad de Control Patrimonial y Bienes	2
Gerencia de Administración y Finanzas	2
Gerencia de Planeamiento y Presupuesto	3
Gerencia de Desarrollo Económico	3
Gerencia de Servicios Públicos	5

Gerencia de Desarrollo Humano	4
Gerencia de Infraestructura, Acondicionamiento Territorial y Catastro	4
TOTAL	**30**

Fuente: Elaboración Propia.

4.4. Definición operacional de las variables en estudio

Tabla Nro. 6: Matriz de operacionalización de la variable.

Variable	Definición conceptual	Dimensiones	Indicadores	Escala de medición	Definición operacional
Propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001	**Definición de diseño** Las políticas de seguridad de información son normas que se establecen y ayuda como guía para las personas de la organización a resguardar correctamente la seguridad de la información. Peltier T. (47), en su libro "Fundamentos de seguridad de la información", considera a la	Satisfacción con la seguridad de información actual.	- Políticas de privacidad para la información. - Cumplen con la práctica de estas políticas de Seguridad. - Medidas del proceso de seguridad de la información. - Inadecuado uso de herramientas de seguridad para actividades TI. - Riesgos que se presentan en los recursos de Información. - Protección física de sus equipos de cómputo. - Incidencias frecuentes por parte de los trabajadores. - Control y manejo de la seguridad de la información. - Satisfacción en la gestión de seguridad. - Fomentar labores políticas en los sistemas de Información.	Ordinal	SI NO

	política como la piedra angular de la arquitectura de seguridad de la información de una organización, ya que de ella nacen otros documentos o declaraciones importantes tales como directivas, estándares, procedimientos y guías.				
		Necesidad de la propuesta de un sistema de la información con normas ISO 2700.	- Capacitación sobre seguridad de la información con Norma ISO 27001. - Desarrollo originalmente en la seguridad informática. - Incorporar una gestión administrativa con la seguridad de la información. - Calidad de servicio para las buenas prácticas en la seguridad de la información. - Monitoreo de la actividad en la seguridad informática. - Reportes en situaciones de pérdidas de información. - Existen divulgación ilícita de la información. - Experiencia de instalaciones de programas. - Control de seguridad en los medios de almacenamiento de información. - Garantía de la propuesta en la Municipalidad.		SI NO

Fuente: Elaboración propia.

4.5. Técnicas e instrumentos de recolección de datos.

4.3.1. Técnica

La técnica que se manejo es la encuesta

Encuesta: Es el conjunto de preguntas especialmente diseñadas y pensadas para ser dirigidas a una muestra de población, que se considera por determinadas circunstancias funcionales al trabajo, representativa de esa población, con el objetivo de conocer la opinión de la gente sobre determinadas cuestiones corrientes y porque no también para medir la temperatura de la gente acerca de algún hecho específico que se sucede en una comunidad determinada y que despierta especial atención entre la opinión pública y que capaz requiere de la realización de una encuesta para conocer más a fondo cuál es la sensación de la gente (48)**.**

4.3.2. Instrumentos

El instrumento que se utilizo es el cuestionario

Cuestionario: Es un procedimiento considerado clásico en las ciencias sociales para la obtención y registro de datos. Su versatilidad permite utilizarlo como instrumento de investigación y como instrumento de evaluación de personas, procesos y programas de formación. Es una técnica de evaluación que puede abarcar aspectos cuantitativos y cualitativos. Su característica singular radica en que, para registrar la información solicitada a los mismos sujetos, ésta tiene lugar de una forma menos profunda e impersonal, que el "cara a cara" de la entrevista. Al mismo tiempo, permite consultar a una población amplia de una manera rápida y económica (49)**.**

4.6. Plan de análisis

La información recopilada será procesada, tabulada y presentada empleando la estadística, para lo cual se elaborarán gráficos y tablas de distribución estadística definida. El procesamiento de los datos se realizó utilizando el programa informático Microsoft Excel 2016. Para el análisis de los datos se utilizó la estadística descriptiva, como tablas de distribución de frecuencia y porcentuales; los resultados serán analizados de acuerdo al comportamiento de las variables respecto a los elementos de estudio, detallado las cifras o resultados más trascendentales de la información correspondiente.

4.7. Matriz de consistencia

Problema	Objetivo general	Hipótesis general	Variables	Metodología
¿De qué manera la propuesta de un Sistema de Gestión de Seguridad de la Información con Normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017, permitirá minimizar la pérdida de información?	Realizar una propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017, de tal forma minimice la pérdida de información.	La propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001, permite minimizar la pérdida de información de la Municipalidad Distrital de Buena Vista Alta – Casma; 2017.	Propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001	Investigación no experimental de tipo descriptivo y de nivel de investigación será de un enfoque cuantitativo.
	Objetivos específicos	Hipótesis específicas		
	1. Analizar la seguridad actual de la información, en la Municipalidad Distrital de Buena Vista Alta - Casma.	1. El análisis de seguridad de la información permite conocer la situación actual de la Municipalidad Distrital de Buena Vista Alta.		

	2. Evaluar los marcos de referencias que ayuden a mejorar la seguridad de la información en la Municipalidad Distrital de Buena Vista Alta - Casma. 3. Proponer la aplicación de la Norma ISO / IEC 27001, para mejorar la seguridad de la información en la Municipalidad Distrital de Buena Vista Alta - Casma.	2. La evaluación de los marcos de referencia permite una mejor seguridad de la información en la Municipalidad Distrital de Buena Vista. 3. La Propuesta de la aplicación de la Norma ISO/IEC 27001, asegura con seguridad de la información en la Municipalidad Distrital de Buena Vista Alta.		

Fuente: Elaboración Propia.

4.8. Principios éticos

Durante el desarrollo de la presente investigación denominada Propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad de Buena Vista Alta se ha considerado en forma estricta el cumplimiento de los principios éticos que permitan asegurar la originalidad de la Investigación. Asimismo, se han respetado los derechos de propiedad intelectual de los libros de texto y de las fuentes electrónicas consultadas, necesarias para estructurar el marco teórico.

Protección a las personas: En el ámbito de la investigación se necesitan cierto grado de protección, que será determinado de acuerdo con el riesgo que incurren y la posibilidad de obtener un beneficio (50).

Beneficencia y no maleficencia: El comportamiento del investigador debe responder a las siguientes reglas generales: causar daño, reducir los efectos negativos y maximizar los beneficios.

Justificación: El investigador debe realizar una evaluación razonable y convincente y tomar las precauciones necesarias para garantizar que sus prejuicios y limitaciones en sus habilidades y conocimientos no conduzcan ni toleren prácticas desleales.

Integridad científica: La integridad del investigador es particularmente relevante al evaluar y explicar los daños, los riesgos y los beneficios potenciales que pueden afectar a quienes participan en una investigación, de acuerdo con los estándares deontológicos de su profesión.

Consentimiento informado y expreso: En toda investigación debe tener la expresión de la voluntad, informada, libre, inequívoca y específica.

V. RESULTADOS

5.1. Resultados

5.1.1. **Dimensión 01:** Satisfacción con la seguridad de información actual.

Tabla Nro. 7:Políticas de privacidad para la información.

Porcentaje y frecuencia relacionadas con los procesos existentes de las políticas de seguridad técnica para la información privada; para la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017.

Alternativas	n	%
Si	6	20.00
No	24	80.00
Total	30	100.00

Fuente: Aplicación del instrumento a los trabajadores de la Municipalidad Distrital de Buena Vista Alta; en relación a la pregunta: ¿Está de acuerdo con el servicio estable y orden de información para mayor seguridad en los sistemas de información?

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro. 7, que el 80.00% de los trabajadores encuestados manifestaron que NO tienen conocimiento sobre lo que significa el servicio estable y orden de información para mayor seguridad en los sistemas de información, mientras que el 20.00% indico que SI están de acuerdo.

Tabla Nro. 8:Cumplen con la práctica de estas políticas de Seguridad.

Porcentajes y frecuencias relacionadas con el análisis de la primera pregunta si brinda mayor cumplimiento con la práctica de estas políticas de seguridad; para la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017.

Alternativas	n	%
Si	12	40.00
No	18	60.00
Total	30	100.00

Fuente: Aplicación del instrumento a los trabajadores de la Municipalidad Distrital de Buena Vista Alta; en relación a la pregunta: ¿Usted cree que cumple con la práctica de estas políticas de seguridad para mayor énfasis en la información?

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro.8, que el 60.00% de los trabajadores encuestados manifestaron que, No se cumplen con las políticas de seguridad, mientras que el 40.00% de los encuestados SI se cumple lo hace a veces en la toma de estas políticas como mejores prácticas de seguridad.

Tabla Nro. 9: Medidas del proceso de seguridad de la información.

Porcentajes y frecuencias relacionadas con la aprobación del acceso de la información para una mayor medida con la seguridad de la información; para la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017.

Alternativas	n	%
Si	25	83.33
No	5	16.67
Total	30	100.00

Fuente: Aplicación del instrumento a los trabajadores de Municipalidad Distrital de Buena Vista Alta; en relación a la pregunta: ¿Cree usted que las medidas del proceso de seguridad de la información son confiables para el acceso de la información?

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro.9, que el 83.33% de los trabajadores encuestados manifestaron que, SI creen al desarrollo de las medidas de seguridad para lograr cambios importantes para el acceso de la información, mientras que el 16.67% de los encuestados NO cree que se logrará un cambio con la medida aprobada para la seguridad de información.

Tabla Nro. 10: Inadecuado uso de herramientas de seguridad para actividades TI.

Porcentajes y frecuencias relacionadas con la utilidad y conocimiento sobre las herramientas de seguridad ante los errores en cualquier proceso de actividad; para la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017.

Alternativas	n	%
Si	4	13.33
No	26	86.67
Total	30	100.00

Fuente: Aplicación del instrumento a los trabajadores de la Municipalidad Distrital de Buena Vista Alta; en relación a la pregunta: ¿Usted tiene conocimiento sobre el uso de las herramientas de seguridad ante los softwares?

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro.10, que el 86.67% de los trabajadores encuestados manifestaron que NO obtienen conocimiento del uso de herramientas de seguridad ante programas que son vulnerables, mientras que el 13.33% de los encuestados SI tienen conocimiento del uso de software de seguridad para la información.

Tabla Nro. 11: Riesgos que se presentan en los recursos de Información.

Porcentajes y frecuencias relacionadas con los informes importantes ante la pérdida de datos frecuentes que presentan riesgos; para la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017.

Alternativas	n	%
Si	20	66.67
No	10	33.33
Total	30	100.00

Fuente: Aplicación del instrumento a los trabajadores de la Municipalidad Distrital de Buena Vista Alta; en relación a la pregunta: ¿Existen riesgos de perdida de datos en los recursos de información en la seguridad de los usuarios?

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro.11, que el 66.67% de los trabajadores encuestados manifestaron que, SI están de acuerdo en que sucede riesgos en pocas veces, pero pierden sus recursos informáticos, mientras que el 33.33% de los encuestados NO presentan casos de riesgos de pérdida de recursos de información.

Tabla Nro. 12: Protección física de sus equipos de cómputo.

Porcentajes y frecuencias relacionadas con la propuesta de conocimiento de protección de equipos ante incidentes de cortes eléctrico para no tener problemas en la perdida de información; para la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017.

Alternativas	n	%
Si	5	16.67
No	25	83.33
Total	30	100.00

Fuente: Aplicación del instrumento a los trabajadores de la Municipalidad Distrital de Buena Vista Alta; en relación a la pregunta: ¿Usted obtienen una buena protección física de sus equipos ante incidentes?

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro.12, que el 83.33.00% de los trabajadores encuestados manifestaron que, NO obtienen instalaciones de protección de sus equipos ante incidentes en las perdidas de su información en la Municipalidad, mientras que el 16.67% de los encuestados SI obtienen la protección por igual por motivos de recursos económicos estarían dispuestos a la pérdida de su información establecida.

Tabla Nro. 13: Incidencias frecuentes por parte de los trabajadores.

Porcentajes y frecuencias relacionadas con respecto a incidencias como perdidas de copias de respaldo de información para mayor seguridad por motivos en fallos eléctricos etc.; para la Propuesta de un servicio estable y orden de información para mayor seguridad en los sistemas de información en la Municipalidad Distrital de Buena Vista Alta. - Casma; 2017.

Alternativas	n	%
Si	24	80.00
No	6	20.00
Total	30	100.00

Fuente: Aplicación del instrumento a los trabajadores de la Municipalidad Distrital de Buena Vista Alta; en relación a la pregunta: ¿Hay frecuencias de incidencias de fallos en la Municipalidad dañando los equipos de cómputo?

Aplicado por: Colonia, P; 2018.

Se observa en los resultados de la Tabla Nro.13, que el 80.00% de los trabajadores encuestados manifestaron que NO hay con frecuencias incidentes muy fuertes para no causar pérdidas de copias de respaldo de información, mientras que el 20.00% indican que, SI existe, pero no tan continua la frecuencia que obtuvieron una pérdida de datos del servidor de la Municipalidad.

Tabla Nro. 14: Control y manejo de la seguridad de la información.

Porcentajes y frecuencias relacionadas con respecto al proceso de control y manejo de la seguridad de la información ante intrusos informáticos y robo de información dentro en los equipos de la Municipalidad teniendo en cuenta la norma ISO 27001; para la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017.

Alternativas	n	%
Si	7	23.33
No	23	76.67
Total	30	100.00

Fuente: Aplicación del instrumento a los trabajadores de la Municipalidad Distrital de Buena Vista Alta; en relación a la pregunta: ¿Usted cree que hay control y manejo en los procesos de actividades privadas para hacer una protección sobre una copia de seguridad de la información?

Aplicado por: Colonia, P; 2018.

Se observa en los resultados de la Tabla Nro.14, que el 76.67% de los trabajadores encuestados manifestaron que NO cuenta con el control y manejo necesario para su seguridad en la parte de proteger datos

informáticos teniendo un riesgo en los sistemas de información, mientras que el 23.33% indican que SI obtienen una protección propia ante los riesgos de la información.

Tabla Nro. 15: Satisfacción en la gestión de seguridad.

Porcentajes y frecuencias relacionadas con el plan de la gestión de seguridad y el proceso de información en la Municipalidad con el fin de definir un impacto económico; para la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017.

Alternativas	n	%
Si	8	26.67
No	22	73.33
Total	30	100.00

Fuente: Aplicación del instrumento a los trabajadores de la Municipalidad Distrital de Buena Vista Alta; en relación a la pregunta: ¿Usted está satisfecho con el proceso de la gestión de una propuesta de seguridad de información?

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro.15, que el 73.33% de los trabajadores encuestados manifestaron que NO están conforme, en lo cual no clasifica para la seguridad de la información, mientras que el 26.67% indican que SI están conforme con la gestión aplicada.

Tabla Nro. 16: Fomentar labores políticas en los sistemas de Información.

Porcentajes y frecuencias relacionadas con la política de seguridad obteniendo una información; para la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017.

Alternativas	n	%
Si	3	10.00
No	27	90.00
Total	30	100.00

Fuente: Aplicación del instrumento a los trabajadores de la Municipalidad Distrital de Buena Vista Alta; en relación a la pregunta: ¿Los sistemas de información permiten una gestión adecuada de los procesos de la Municipalidad?

Aplicado por: Colonia, P; 2018.

Se observa en los resultados de la Tabla Nro.16, que el 90.00% de los trabajadores encuestados manifestaron que NO fomentan labores esenciales a las políticas en los sistemas de información, mientras que el 10.00% indica que SI hacen unas propuestas sobre las labores políticas en casos importantes.

5.1.2. **Dimensión 02:** Necesidad de la propuesta de un sistema de la información con normas ISO 27001.

Tabla Nro. 17: Capacitación sobre seguridad de la información con Norma ISO 27001.

Porcentajes y frecuencias relacionadas con la capacitación sobre la seguridad de los sistemas de información en eventos o taller para mayor experiencia; para la Propuesta de un servicio estable y orden de información para mayor seguridad en los sistemas de información en la Municipalidad Distrital de Buena Vista Alta. - Casma; 2017.

Alternativas	n	%
Si	30	100.00
No	-	-
Total	30	100.00

Fuente: Aplicación del instrumento a los trabajadores de la Municipalidad Distrital de Buena Vista Alta; en relación a la pregunta: ¿Cree usted que la capacitación le ayudara a tomar conciencia lo importante que es la seguridad de la información con Normal ISO 27001?

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro.17, que el 100.00% de los trabajadores encuestados manifestaron que, SI tiene capacitaciones mensuales para dar a conocer sobre la Norma ISO 27001 con el proceso de la gestión de seguridad de la información, mientras que ningún trabajador indico lo contrario.

Tabla Nro. 18: Desarrollo originalmente en la seguridad informática.

Porcentajes y frecuencias relacionadas con la seguridad informática para destacar perdido de información en los equipos de cómputo con un diseño de protección en software y en las redes informática; para la Propuesta de un servicio estable y orden de información para mayor seguridad en los sistemas de información en la Municipalidad Distrital de Buena Vista Alta. - Casma; 2017.

Alternativas	n	%
Si	6	20.00
No	24	80.00

Total	30	100.00

Fuente: Aplicación del instrumento a los trabajadores de la Municipalidad Distrital de Buena Vista Alta; en relación a la pregunta: ¿Usted cree que la seguridad informática está desarrollada sin pensar originalmente en la protección de la información?

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro.18, que el 80.00% de los trabajadores encuestados manifestaron que NO cuenta con un desarrollo originalmente en la protección de sus datos informáticos de información de proyecto u otras gestiones municipales, mientras que el 20.00% indica que SI obtienen un desarrollo particular propio que guardan su información de manera segura con software libre que no son originales.

Tabla Nro. 19: Incorporar una gestión administrativa con la seguridad de la información.

Porcentajes y frecuencias relacionadas con el total del personal administrativo de TI considera una gestión de seguridad de la información en la gestión administrativa es buena; para la Propuesta de un servicio estable y orden de información para mayor seguridad en los sistemas de información en la Municipalidad Distrital de Buena Vista Alta. - Casma; 2017.

Alternativas	n	%

Si	30	100.00
No	-	-
Total	30	100.00

Fuente: Aplicación del instrumento aplicado a los trabajadores de la Municipalidad Distrital de Buena Vista Alta; en relación a la pregunta: ¿Usted aprueba la gestión administrativa para el proceso de una buena gestión de seguridad de la información?

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro.19, que el 100.00% de los trabajadores encuestados manifestaron que, SI han aceptado la aprobación de una gestión administrativo incorporando la gestión de seguridad de la información, mientras que ningún personal administrativo declaro en contra.

Tabla Nro. 20: Calidad de servicio para las buenas prácticas en la seguridad de la información.

Porcentajes y frecuencias relacionadas apuesta por una nueva calidad en el servicio de los empleados y administrativos de la Municipalidad para la propuesta de las buenas prácticas; para la Propuesta de un servicio estable y orden de información para mayor seguridad en los

sistemas de información en la Municipalidad Distrital de Buena Vista Alta. - Casma; 2017.

Alternativas	n	%
Si	-	-
No	30	100.00
Total	30	100.00

Fuente: Aplicación del instrumento a los trabajadores de la Municipalidad Distrital de Buena Vista Alta; en relación a la pregunta: ¿Usted aprueba en la calidad de servicio para la mejor propuesta de las buenas prácticas?

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro.20, que el 100.00% aplicado a los trabajadores de NO tienen una buena calidad en el servicio de la seguridad de la información para promover las buenas prácticas, mientras que ningún personal administrativo declaro a favor.

Tabla Nro. 21: Monitoreo de la actividad en la seguridad informática.

Porcentajes y frecuencias relacionadas en comprobar las actividades de la seguridad de la información por medio de monitorios en cada máquina y verificar si cuentan con los softwares adecuados para la protección de los datos de la Municipalidad; para la Propuesta de un servicio estable y orden de información para mayor seguridad en los

sistemas de información en la Municipalidad Distrital de Buena Vista Alta. - Casma; 2017.

Alternativas	n	%
Si	30	100.00
No	-	-
Total	30	100.00

Fuente: Aplicación del instrumento a los trabajadores de la Municipalidad Distrital de Buena Vista Alta; en relación a la pregunta: ¿Cree usted que verificando su equipo de trabajo en la Municipalidad requiere de un monitoreo para determinar la falta de seguridad de información?

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro.21, que el 100.00% de los trabajadores encuestados manifestaron que, SI apoya al monitoreo en todas las máquinas de los trabajadores para resolver la seguridad de la información, mientras que ningún personal administrativo declaro en contra.

Tabla Nro. 22: Reportes en situaciones de pérdidas de información.

Porcentajes y frecuencias relacionadas para el desarrollo de normativas internas y reportes de actividades en la parte de la seguridad informática en situaciones de casos de perdida de información; para la Propuesta de un servicio estable y orden de

información para mayor seguridad en los sistemas de información en la Municipalidad Distrital de Buena Vista Alta. - Casma; 2017.

Alternativas	n	%
Si	8	26.67
No	22	73.33
Total	30	100.00

Fuente: Aplicación del instrumento aplicado a los trabajadores de Municipalidad Distrital de Buena Vista Alta; en relación a la pregunta: ¿Cree usted que la gestión de seguridad de la información confirme los reportes dados en situaciones importante de pérdidas totales de datos en la Municipalidad?

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro.22, que el 73.33% de los trabajadores encuestados manifestaron que NO cuenta con un sistema de reportes de pérdidas de datos en la Municipalidad en el sistema de gestión sobre la seguridad de la información, mientras que el 26.67% declaran que, SI cuenta con reportes, pero pocas en el sistema de seguridad de la información.

Tabla Nro. 23: Existen divulgación ilícita de la información.

Porcentajes y frecuencias relacionadas con la existencia de divulgaciones ilícita de la información por los trabajadores de la Municipalidad; para la Propuesta de un servicio estable y orden de información para mayor seguridad en los sistemas de información en la Municipalidad Distrital de Buena Vista Alta. - Casma; 2017.

Alternativas	n	%
Si	30	100.00
No	-	-
Total	30	100.00

Fuente: Aplicación del instrumento aplicado a los trabajadores de Municipalidad Distrito de Buena Vista Alta; en relación a la pregunta: ¿Cree usted que el análisis de las divulgaciones ilícitas en la Municipalidad se tomara en cuenta la propuesta de la seguridad de la información?

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro.23, que el 100.00% de los trabajadores encuestados manifestaron que, SI sucede divulgaciones ilícitas por gestiones realizados en la Municipalidad y requiere una seguridad máxima con el entono a su información tomando en cuenta la norma ISO 27001, mientras que ningún personal administrativo declaro en contra.

Tabla Nro. 24: Experiencia de instalaciones de programas.

Porcentajes y frecuencias relacionadas que permitirán la experiencia para cada trabajador obtener un proceso de instalación de programas para mantener casos vulnerables en los equipos de la Municipalidad;

para la Propuesta de un servicio estable y orden de información para mayor seguridad en los sistemas de información en la Municipalidad Distrital de Buena Vista Alta. - Casma; 2017.

Alternativas	n	%
Si	18	60.00
No	12	40.00
Total	30	100.00

Fuente: Aplicación del instrumento aplicado a los trabajadores de Municipalidad Distrito de Buena Vista Alta; en relación a la pregunta: ¿Usted tiene experiencia sobre instalaciones de programas ante las vulnerabilidades que ocasionan en los sistemas informáticos para la seguridad de la información?

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro.24, que el 60.00% de los trabajadores encuestados manifestaron que SI tiene experiencia en temas de la informativa cabe destacar que estas especializados en la toma de instalaciones de programas para anteponer problemas sobre la información de la Municipalidad, mientras que el 40.00% indican que NO tienen experiencia en temas de ese tipo de uso.

Tabla Nro. 25: Control de seguridad en los medios de almacenamiento de información.

Porcentajes y frecuencias relacionadas que obteniendo un control de seguridad en los medios de almacenamiento de información en la Municipalidad para conseguir la seguridad calificada y determinar copias seguras de sus datos; para la Propuesta de un servicio estable y

orden de información para mayor seguridad en los sistemas de información en la Municipalidad Distrital de Buena Vista Alta. - Casma; 2017.

Alternativas	n	%
Si	30	100.00
No	-	-
Total	30	100.00

Fuente: Aplicación del instrumento aplicado a los trabajadores de Municipalidad Distrito de Buena Vista Alta; en relación a la pregunta: ¿Usted cree que teniendo un control de medios de almacenamiento de datos resguardara la seguridad de información en la Municipalidad?

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro.25, que el 100.00% de los trabajadores encuestados manifestaron que, SI están conforme sobre la propuesta del control de medios de almacenamiento de información para mejorar la seguridad en el entono de sus informes, mientras que ningún personal administrativo declaro en contra.

Tabla Nro. 26: Garantía de la propuesta en la Municipalidad.

Porcentajes y frecuencias relacionadas con el fin de garantizar la seguridad de la información con esta propuesta dada para la comodidad y confianza en casos de perdida de datos para cada

trabajador; para la Propuesta de un servicio estable y orden de información para mayor seguridad en los sistemas de información en la Municipalidad Distrital de Buena Vista Alta. - Casma; 2017.

Alternativas	n	%
Si	30	100.00
No	-	-
Total	30	100.00

Fuente: Aplicación del instrumento aplicado a los trabajadores de Municipalidad Distrito de Buena Vista Alta; en relación a la pregunta: ¿Cree usted que la propuesta garantizara la mejora en los recursos de la seguridad de la información en la Municipalidad?

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro.26, que el 100.00% de los trabajadores encuestados manifestaron que, SI están confiados y aceptando el uso de esta propuesta tomando en cuenta la garantía para la seguridad de su información protegida, mientras que ningún personal administrativo declaro en contra.

5.2. Resultado por dimensión

Tabla Nro. 27:Satisfacción con la seguridad de información actual.

Porcentajes y frecuencias relacionadas con la dimensión 01: Satisfacción con la seguridad de información actual; respecto a la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017.

Alternativas	n	%
Si	8	26.67
No	22	73.33
Total	30	100.00

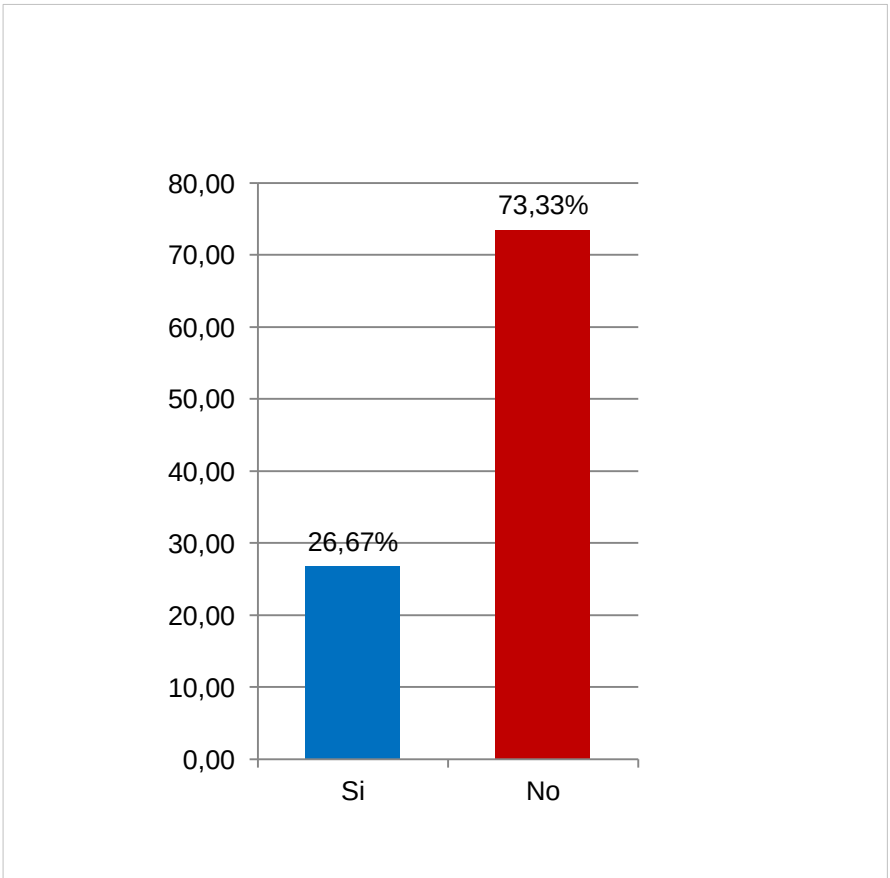
Fuente: Aplicación del instrumento en relación a medir la dimensión: Satisfacción con la seguridad de información actual, basado en diez preguntas aplicadas a los trabajadores de la Municipalidad Distrito de Buena Vista Alta. - Casma; 2017.

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro.27, que el 73.33% de los trabajadores encuestados expresaron NO están satisfechos con el sistema de información actual; mientras el 26.67% indicó que SI se encuentran satisfechos con respecto al sistema actual.

Gráfico Nro. 8: Satisfacción con la seguridad de información actual.

Distribución porcentual de frecuencias y respuestas relacionadas con la dimensión 01: Satisfacción con la seguridad de información actual; respecto a la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017.



Fuente: Tabla Nro.27: Satisfacción con la seguridad de información actual.

Tabla Nro. 28: Necesidad de la propuesta de un sistema de la información con normas ISO 27001.

Porcentajes y frecuencias relacionadas con la dimensión 02: Necesidad de la propuesta de un sistema de la información con normas ISO 27001; respecto a la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017.

Alternativas	n	%
Si	30	100.00
No	-	-
Total	30	100.00

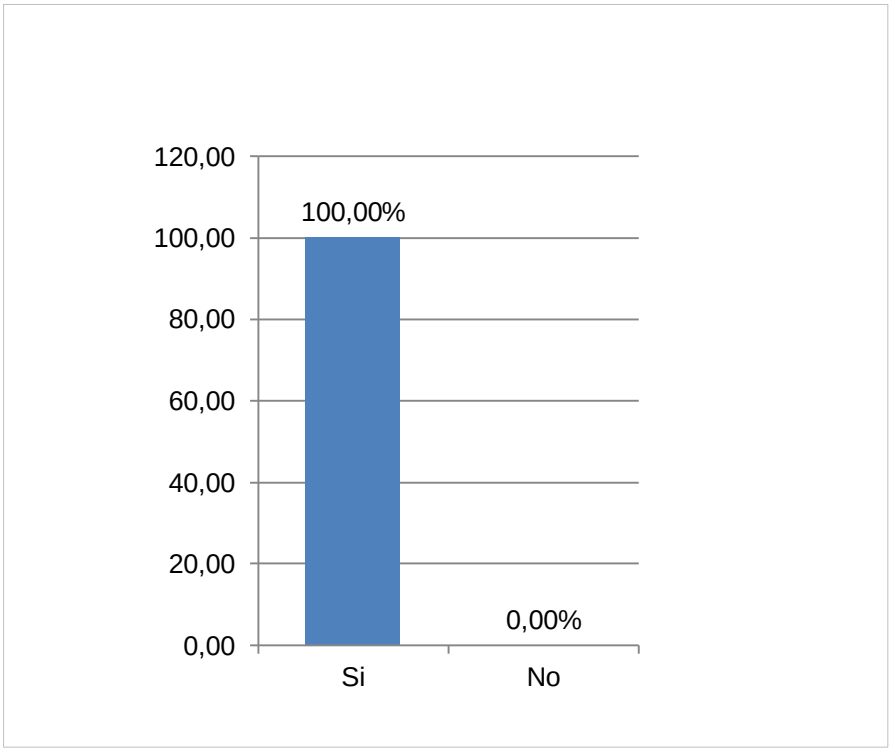
Fuente: Aplicación del instrumento en relación a medir la dimensión: Necesidad de la propuesta de un sistema de la información con normas ISO 27001, basado en diez preguntas aplicadas a los empleados y administrativos de la Municipalidad Distrital de Buena Vista Alta. - Casma; 2017.

Aplicado por: Colonia, P.; 2018.

Se observa en los resultados de la Tabla Nro.28, que el 100.00% de los trabajadores encuestados expresaron SI se encuentran con la necesidad de la propuesta de un sistema de la información con normas ISO 27001.

Gráfico Nro. 9: Necesidad de la propuesta de un sistema de la información con normas ISO 27001.

Porcentajes y frecuencias relacionadas con la dimensión 02: Necesidad de la propuesta de un sistema de la información con normas ISO 27001; respecto a la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad de Buena Vista Alta – Casma; 2017.



Fuente: Tabla Nro.28: Necesidad de la propuesta de un sistema de la información con normas ISO 27001.

.

Tabla Nro. 29: Resumen General de Dimensiones

Porcentajes y frecuencias relacionadas con las dos dimensiones planteadas para determinar los niveles de satisfacción del actual sistema y de la necesidad de una propuesta de mejora, aplicada a los empleados respecto; a la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad de buena vista alta – casma; 2017.

DIMENSIONES	ALTERNATIVAS DE RESPUESTA				MUESTRA	
	Si	%	No	%	n	%
Satisfacción con la seguridad de información actual.	8	26.67	22	73.33	30	100.00
Necesidad de la propuesta de un sistema de la información con normas ISO 27001.	30	100.00	-	-	30	100.00

Fuente: Aplicación del instrumento a los trabajadores encuestados acerca de la satisfacción de las dos dimensiones definidas para la investigación relacionadas con la satisfacción con la seguridad de información actual y la necesidad de la propuesta de un sistema de la información con normas ISO 27001 para la Municipalidad Distrital de

Buena Vista Alta – Casma; 2017.

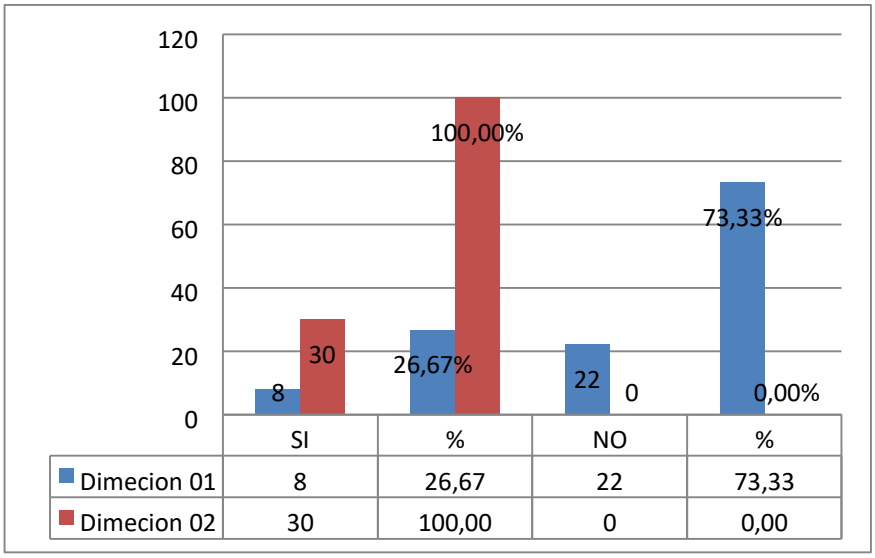
Aplicado por: Colonia, P.; 2018.

En los resultados de la Tabla Nro. 29, se puede observar que en lo que respecta a la dimensión 01: satisfacción con la seguridad de información actual el 73.33% de los trabajadores encuestados determinó que NO están satisfechos con el seguridad de información actual y en lo que se concierne a la dimensión 02 necesidad de la propuesta de un sistema de la información con normas ISO 27001 el 100.00% concluyó indicando que SI están de acuerdo a la necesidad de la propuesta de un sistema de la información con normas ISO 27001.

Gráfico Nro. 10: Resumen general de dimensiones

Porcentajes y frecuencias de las respuestas relacionadas con las dos dimensiones planteadas para determinar la Satisfacción con la seguridad de información actual y la Necesidad de la propuesta de un sistema de la información con normas ISO 27001; a la propuesta de un sistema de gestión de seguridad de la información con normas ISO

27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017.

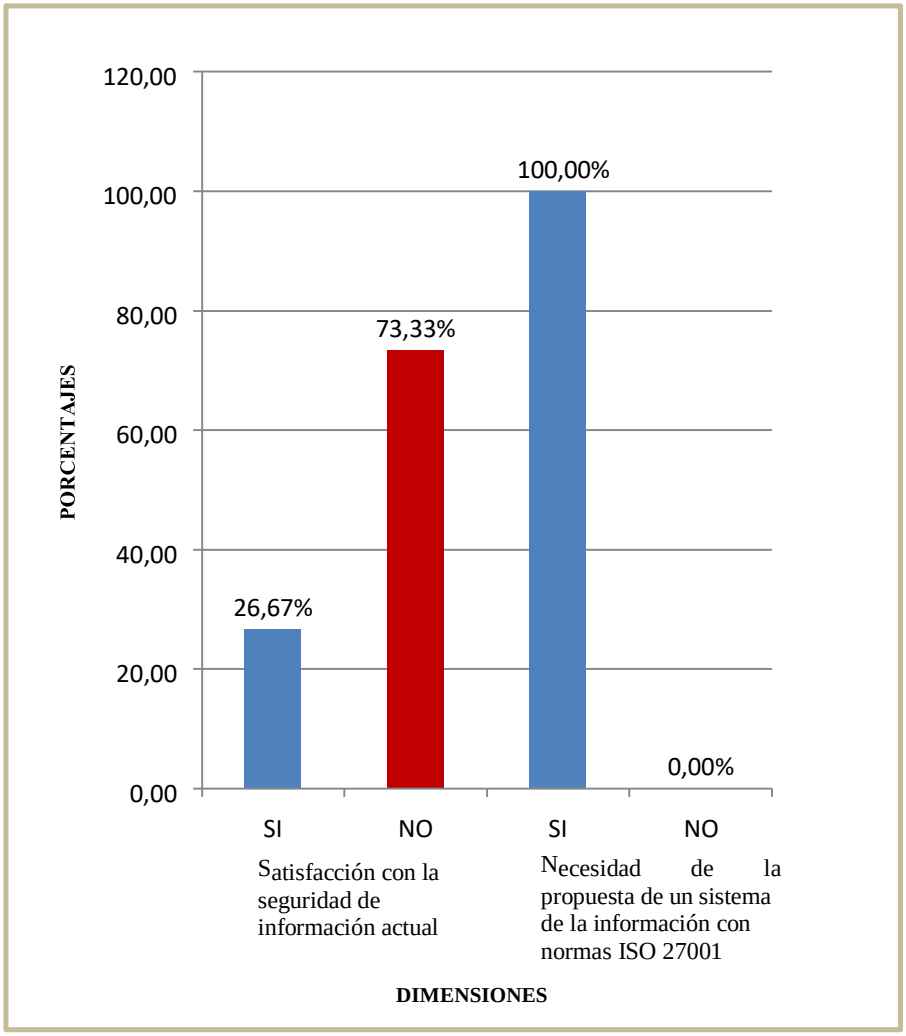


	SI	%	NO	%
Dimecion 01	8	26,67	22	73,33
Dimecion 02	30	100,00	0	0,00

Fuente: Tabla Nro.29: Resumen General de Dimensiones

Gráfico Nro. 11: Resumen Porcentual de Dimensiones.

Porcentajes y frecuencias de las respuestas relacionadas con las dos dimensiones planteadas para determinar la Satisfacción con la seguridad de información actual y la Necesidad de la propuesta de un sistema de la información con normas ISO 27001, aplicada a los trabajadores y administrativos respecto; a la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad de Buena Vista Alta – Casma; 2017.



Fuente: Tabla Nro.29: Resumen General de Dimensiones

5.3. Análisis de resultados

La presente investigación tuvo como objetivo general: Realizar la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma;2017 con el fin de minimizar el riesgo de pérdida de información; para cumplir este objetivo, fue necesario evaluar la situación actual para que este diseño identifique claramente los requisitos que permiten la protección de la información dirigida a mantener la confidencialidad, accesibilidad e integridad del mismo genoma de una propuesta de definidas mejora seria y técnica. Se ha tenido que realizar la aplicación del instrumento que permita conocer la percepción de los trabajadores frente a las dos dimensiones para esta encuesta. En

consecuencia, luego de la interpretación de los resultados realizada en la sección anterior se puede realizar los siguientes análisis de resultados.

1. En relación a la dimensión 01: Satisfacción con la seguridad de información actual en la Tabla Nro. 27 nos muestra los resultados donde se puede observar que el 73.33% de los trabajadores encuestados expresaron NO están satisfechos con el sistema de información actual, por ese motivo damos en cuenta la importancia de la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 que permita minimizar los riesgos y amenazas en seguridad de información. Estos resultados se asemejan a los obtenidos por Guamán J. (3), en su tesis titulada "Diseño de un sistema de gestión de seguridad de la información para instituciones militares", en la ciudad de Quito – Ecuador. Donde sus resultados son similares a la presente dimensión, debido a que obtuvo un 56,86% de aceptación de su población en la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 en la empresa ya que permite una mejor seguridad de la información en las diversas áreas tecnológicas de la empresa, por lo cual se justifica que ambos resultados tienen la necesidad de mejorar la seguridad de información y por ende impedir la pérdida y eliminación de información que le pertenecen a la empresa. Concluyendo que, establecer objetivos de control de seguridad a través de la norma ISO 27001, dará un mejor sostén en la gestión de las tecnologías de la información y la comunicación en la empresa.

2. Con respecto a la 02: Necesidad de la propuesta de un sistema de la información con normas ISO 27001, en la Tabla Nro.28, nos muestra que el 100.00% de los trabajadores encuestados expresaron SI se encuentran

con la necesidad de la propuesta de un sistema de la información con normas ISO 27001,donde estos resultados se asemejan al obtenido por Bermúdez, K. y C Bailón, E. (4), en la tesis "Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001 – sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros", en la ciudad de Ecuador. Debido a que obtuvo como resultados un nivel de incidencia del 95.65% al no contar con una Política de Normalización de la Seguridad de Información que pueda impedir la perdida y eliminación de información que le pertenece a la empresa, por lo cual se justifica que ambos resultados tienen la necesidad de establecer una Política de Seguridad de Información en la plataforma tecnológica de la empresa las cuales deben estar documentadas y deben ser de conocimiento de todos los empleados. Concluyendo que, es necesario establecer una Política de Seguridad de Información que contenga los lineamientos para una eficiente administración de la información con el fin de garantizar la seguridad de los sistemas que satisfaga el requerimiento del negocio y de mantener la integridad de la información, de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad.

5.3. Propuesta de mejora

Habiéndose realizado el análisis de los datos recogidos a través de la evaluación de los dominios: Satisfacción de la seguridad de la información y la necesidad de mejorar la seguridad de la información. Se propone la aplicación de la norma ISO / IEC 27001, el mismo que permitirá mejora los siguientes procesos:

- Establecer políticas de seguridad, con respecto a la adquisición, distribución y uso de las TI en la Municipalidad Distrital de Buena Vista Alta.
- Que la Alta gerencia, muestre compromiso con las innovaciones tecnológicas que soportan los procesos de la Municipalidad Distrital de Buena Vista Alta.
- Determinar procesos que aseguren la Seguridad de la información en la Municipalidad Distrital de Buena Vista Alta.
- Establecer procedimientos que aseguren la confidencialidad de la información en la Municipalidad Distrital de Buena Vista Alta.
- Establecer políticas que aseguren la factibilidad y protección de brindar información a terceros.
- Definir procesos documentados para el registro de inventarios de activos de TI en la Municipalidad Distrital de Buena Vista Alta.
- Realizar el registro automatizado de la asignación de responsables de activos de TI en la Municipalidad Distrital de Buena Vista Alta.
- Determinar los roles y responsabilidades del personal de TI en la Municipalidad Distrital de Buena Vista Alta.
- Establecer las responsabilidades de los usuarios que hacen uso de las TI de acuerdo a las funciones establecidas en la Municipalidad Distrital de Buena Vista Alta.
- Planificar capacitaciones y entrenamientos al personal que utiliza las TI en la Municipalidad Distrital de Buena Vista Alta.
- Documentar las políticas para sanciones por uso indebido de los sistemas de información.

- Definir los procesos de seguridad de ambientes físicos y ambientales para los activos de TI en la Municipalidad Distrital de Buena Vista Alta.
- Determinar los procesos para operaciones y transacciones de TI que realiza las unidades operativas de la Municipalidad Distrital de Buena Vista Alta.
- Definir los procesos para solicitudes y atención de soporte de TI en la Municipalidad Distrital de Buena Vista Alta.

De acuerdo a la investigación se ha seleccionado la Norma ISO 27001:2013, nos muestra que existe la necesidad de mejorar el sistema de gestión de la seguridad de la información, por lo cual se propone las siguientes preguntas:

Tabla Nro. 30: Tabla de evaluación del sistema de gestión de seguridad.

El presente formulario es para evaluar el nivel de madurez que se encuentra la seguridad de la información, según los controles definidos en la ISO/IEC 27001:2013.			
Objetivo de Control	Controles	Verificación	
		SI	NO
Política de Seguridad	Se verifica las políticas de seguridad de información.		
	Existen Perfiles que asegure la seguridad de la información.		
	La alta gerencia está comprometida con la seguridad de la información.		
	Existe coordinación entre la gerencia de TI y las otras áreas a fin de mejorar la seguridad de información.		
	Existen asignación de responsabilidades, respecto a la seguridad de la información.		
	Se establece los procesos de autorización para los cambios de procesamiento de información.		

	Se evidencias normas de confidencialidad.		
	Existe un proceso de coordinación con autoridades.		
	Existe registro de Contacto de los grupos de interés.		
	Se realiza revisiones periódicas que aseguren la seguridad de la información.		
	Se identifica la existencia de riesgos relacionados con entidades externas.		
	Existe contratos del tratamiento de la seguridad información, cuando se trabaja con clientes.		
	Se evidencia criterios para garantizar la seguridad de la información, frente a terceros.		
Gestión de Activos	Existe inventarios de activos.		
	Los activos, son verificados de manera periódica, para asegurar su estado.		
	Se verifica el uso aceptable de los activos.		
	Se clasifican los activos de acuerdo a categorías.		
	Existe técnicas para la atomización del registro de activos.		
Seguridad de los Recursos Humanos	Se verifica Roles y responsabilidades de los usuarios.		
	Existe un proceso de selección para asignar responsables de las copias de seguridad de información.		
	Se verifica términos y condiciones de empleo.		
	Existe una gestión de Responsabilidades		
	Se planifica capacitación y educación en seguridad de la información		

	Existen procedimientos disciplinarios con respecto a la vulnerabilidad de la seguridad de la información.		
	Se registran las incidencias de vulnerabilidad y/o amenazas de la seguridad de la información.		
	Se evidencia la devolución de activos, por parte del recurso humano cesado o asignado a otras funciones.		

	Se verifica la eliminación de derechos de acceso al usuario cesado.		
Seguridad Física y Ambiental	El perímetro de la seguridad de la información, representa seguridad para los equipos de la seguridad de la información.		
	Existen controles en las entradas de ambientes físicos.		
	Se verifica la seguridad de oficinas, ambientaciones y medios.		
	Existe protección contra amenazas externas, respecto a los ambientes.		
	Se comprueba los trabajos en áreas seguras.		
	Se comprueba las áreas de acceso público, entrega y carga.		
	Se evidencia la ubicación y protección de equipos.		
	Se verifica la existencia de algunos servicios públicos.		
	Existe alguna seguridad en el cableado.		
	Existe mantenimiento de equipo.		
	Existe verificación de seguridad del equipo fuera del local.		
	Se comprueba eliminación segura o rehusó del equipo.		
	Se comprueba el traslado de propiedades.		
Gestión de la Comunicación y Operaciones	Existe procedimientos de operación documentadas.		
	Le verifica gestión de cambio.		
	Existe la segregación de deberes.		

	Se verifica la separación de los medios de desarrollo y operacionales.		
	Existe alguna Entrega de servicios.		
	Se comprueba monitoreo y revisión de los servicios de terceros.		
	Se verifica el majeño de los cambios en los servicios de terceros.		
	Existe alguna gestión de la capacidad.		
	Se comprueba la aceptación del sistema.		
	Existe algún control sobre Software maliciosos.		
	Se evidencia los controles contra códigos móviles.		

	Existen evidencias de Backup o controles de la información.		
	Existe algún control de Red.		
	Se comprueba la seguridad de los servicios de Red.		
	Se verifica la gestión de los medios removibles.		
	Se comprueba la eliminación de medios.		
	Existe algún Procedimientos de los manejos de información.		
	Se comprueba la seguridad de documentación del sistema.		
	Existen procedimientos y políticas de información y Software.		
	Se verifica el registro de acuerdos de intercambios.		
	Se comprueba medios físicos en tránsito.		
	Se verifican los mensajes electrónicos.		
	Existe algunos sistemas de información comercial		

	Existe verificación de registro de comercio electrónico.		
	Se comprueba Transacciones en línea.		
	Se verifica la información disponible públicamente.		
	Existe algún Registro de auditoria		
	Se verifica la existencia del sistema de monitoreo.		
	Existe alguna protección del sistema de monitoreo.		
	Se vírica la protección de la información del registro.		
	Se comprueba los registros del administrador y operador.		
	Existe algún Registro de fallas.		
	Existe verificación de sincronización de relojes.		
	Se comprueba las políticas del control de accesos.		
	Existe alguna inscripción del usuario.		
	Existe una verificación de gestión de privilegios.		
	Existe alguna gestión de clave de usuarios.		
Control de Acceso	Revisión de los accesos de los derechos del usuario.		
	Existe algún uso de clave.		
	Equipamiento de usuario desatendido.		
	Existe alguna política de pantalla y escritorio limpio.		
	Existe alguna política sobre el uso de servicios en Red.		
	Se comprueba Autenticación del usuario para conexiones externas.		
	Se comprueba la identificación del equipo en Red.		
	Existe alguna protección del puerto de diagnóstico remoto.		
	Segregación en redes.		
	Existe algún control de conexiones en redes.		

	Se comprueba el control de routing en redes.		
	Existe algún procedimiento de registro en el terminal.		
	Se verifica la identificación y autenticación del usuario.		
	Se comprueba el sistema de gestión de claves.		
	Se verifica el uso de utilidades del sistema.		
	Existe alguna sesión inactiva.		
	Se comprueba la limitación de tiempo de conexión.		
	Existe alguna restricción al acceso a la información.		
	Existe algún aislamiento del sistema sensible.		
	Se verifica la existencia de computación móvil y comunicación.		
	Existe algún Tele-trabajo.		

Fuente: Elaboración Propia.

La incorporación de los presentes objetos de control, permitirá calcular el nivel de riesgo que considera y las metodologías de otros. Sin embargo, aquí veremos una fórmula simple y rápida para entender, basada en dos parámetros fundamentales en la gestión de riesgos: Probabilidades y Amenazas.

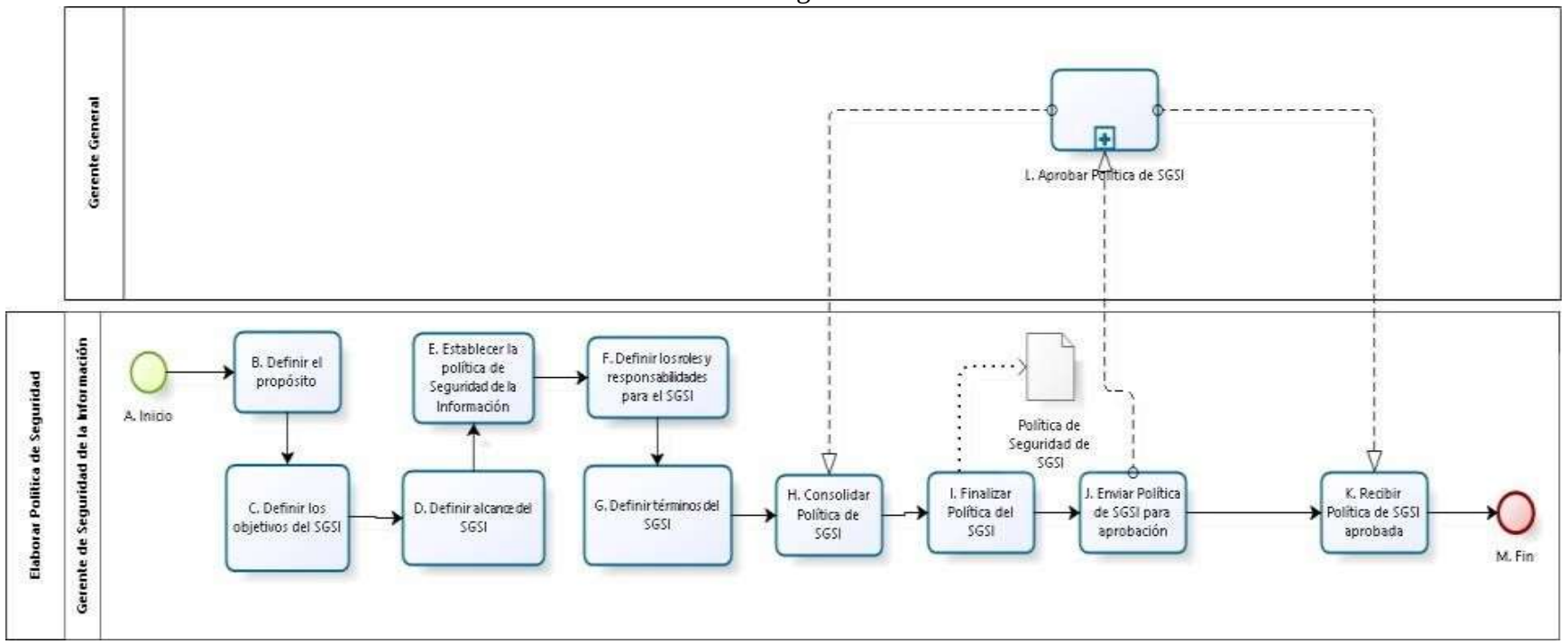
El Plan de Tratamiento de Riesgos debe contener una serie de informaciones básicas: Responsable del control: Persona responsable por la correcta implementación del control, Recursos: Personas, técnicos, empresas externas

o materiales que serán utilizados para la implementación del control, Acciones a realizar: Acciones que serán necesarias para la implementación del control, Prioridad: Todos los controles no tienen la misma prioridad, ya que, por un lado, el nivel de riesgo no será el mismo, ni el valor de cada activo para la Organización. Por lo tanto, es necesario establecer prioridades, que pueden determinarse hasta la fecha de contabilización. implementación de cada control.

Proceso – Elaborar Política de seguridad de la información

A continuación, se presenta el proceso de implementación de la política de seguridad de la información:

Gráfico Nro. 12: Elaborar Política de seguridad de la información.



Fuente: Elaboración Propia.

Una propuesta eficaz para hacer una implementación adecuada de la ISO 27001: 2013, es analizar las fortalezas y debilidades de los elementos más importantes que proponga en la imagen de los gráficos Nro. 13.

Gráfico Nro. 13: Propuesta de Fortalezas y Debilidades de TI.

Fuente: Elaboración Propia.

Para mitigar las vulnerabilidades encontradas se debe definir y priorizar actividades que conlleven a la aplicación del plan de gestión de la seguridad de la información mediante la implementación de controles de seguridad. Para esto se ha considerado las siguientes fases, en las cuales se detallan un conjunto de actividades a ser realizadas por la Municipalidad Distrital de Buena Vista Alta.

Primera Fase:

Esta primera fase comprende el inicio del plan de gestión de la seguridad de la información, donde se establecen responsabilidades, estándares y procedimientos sobre la dirección del plan de gestión de seguridad.

- Designar formalmente al Responsable de Seguridad de la información y/o Seguridad Informática.
- Definir y establecer las responsabilidades y objetivos del Responsable de Seguridad de la información y/o Seguridad Informática.
- Conformar el Comité de Gestión de la Seguridad de la Información.
- Analizar cada una de las recomendaciones dadas, de tal forma que se dé prioridad de implementación a los controles de seguridad que puedan disminuir el riesgo de mayor impacto.
- Diseñar el manual de políticas de seguridad de la información en base a los controles implementados actualmente y considerando nuevos controles que podrán ser implementados dentro de la Municipalidad Distrital de Buena Vista Alta.
- Establecer los procedimientos e instructivos de seguridad.
- Designar formalmente a los Propietarios de los activos de información.

- Elaborar un catálogo de Clasificación de la información por área, el cual debe ponerse en conocimiento de todos los empleados (categorización: confidencial o pública).

- Evaluar con personal especializado todo lo referente a requerimientos legales, tomando en cuenta organismos de control que regulan a la Municipalidad Distrital de Buena Vista Alta, leyes ecuatorianas, entre otros.

Segunda Fase:

Esta fase comprende la aplicación de los controles de seguridad anteriormente definidos, se realizan las actividades que han sido diseñadas con el propósito de disminuir el riesgo actual.

- Crear e implementar un programa de capacitación para los empleados de la Municipalidad Distrital de Buena Vista Alta acerca de temas relacionados con la seguridad informática (charlas, boletines, seminarios, entre otros).

- Implementar los controles de seguridad recomendados en la matriz de situación actual y activos de la información, tomando en cuenta la protección física y lógica de la información y de los sistemas de procesamiento de información.

- Definir y establecer políticas y responsabilidades sobre la administración de accesos de los sistemas de información.

- Estandarizar los user ID, de tal forma que los empleados utilicen un solo usuario para el ingreso a los diferentes aplicativos de la Municipalidad Distrital de Buena Vista Alta.

- Definir y establecer políticas que detallen el buen uso que se le debe dar a los activos de la Municipalidad Distrital de Buena Vista Alta.

- Definir procesos que permitan conocer las responsabilidades y obligaciones de empleados, pasantes, practicantes y terceros en cuanto a la seguridad de la información.
- Gestionar el buen uso de las redes y comunicaciones, generando procedimientos e instructivos.
- Definir el proceso para gestionar los cambios que se necesiten realizar en los aplicativos de la Municipalidad Distrital de Buena Vista Alta.
- Incorporar la seguridad de la información en la Gestión de la continuidad del negocio.
- Administrar y registrar los incidentes de seguridad de la información que se presente.
- Analizar la posibilidad de implementación de sistemas de video vigilancia, detectores de humo, sistemas contra incendios.
- Registrar pistas de auditorías en los sistemas de información de la Municipalidad Distrital de Buena Vista Alta.
- Definir un backup para cada funcionario que desempeñe un rol crítico dentro de las actividades del área de sistemas.

Tercera Fase:

- Monitorear la gestión de seguridad de la información, comprobar su eficacia con la finalidad de poder realizar ajustes al plan de seguridad.
- Monitoreo continuo de los controles de seguridad implementados para prevenir incidentes de seguridad.
- Analizar la posibilidad de adquirir herramientas para monitorear las aplicaciones, redes, códigos maliciosos, entre otros.
- Diseñar y ejecutar los indicadores de gestión de seguridad.

- Monitorear el cumplimiento de la gestión del buen uso de los activos.

- Monitorear el acceso y buen uso de redes y comunicación.
- Monitorear el correcto funcionamiento de servicios prestados por terceros.

- Monitorear el cumplimiento de estándares de seguridad del Data-Center.

- Registrar el resultado de los monitoreos realizados.

Cuarta Fase:

- Mejorar la gestión de seguridad de la información considerando las vulnerabilidades encontradas luego de monitorear el plan vigente.

- Identificar e incorporar mejoras a la gestión de la seguridad de la información.

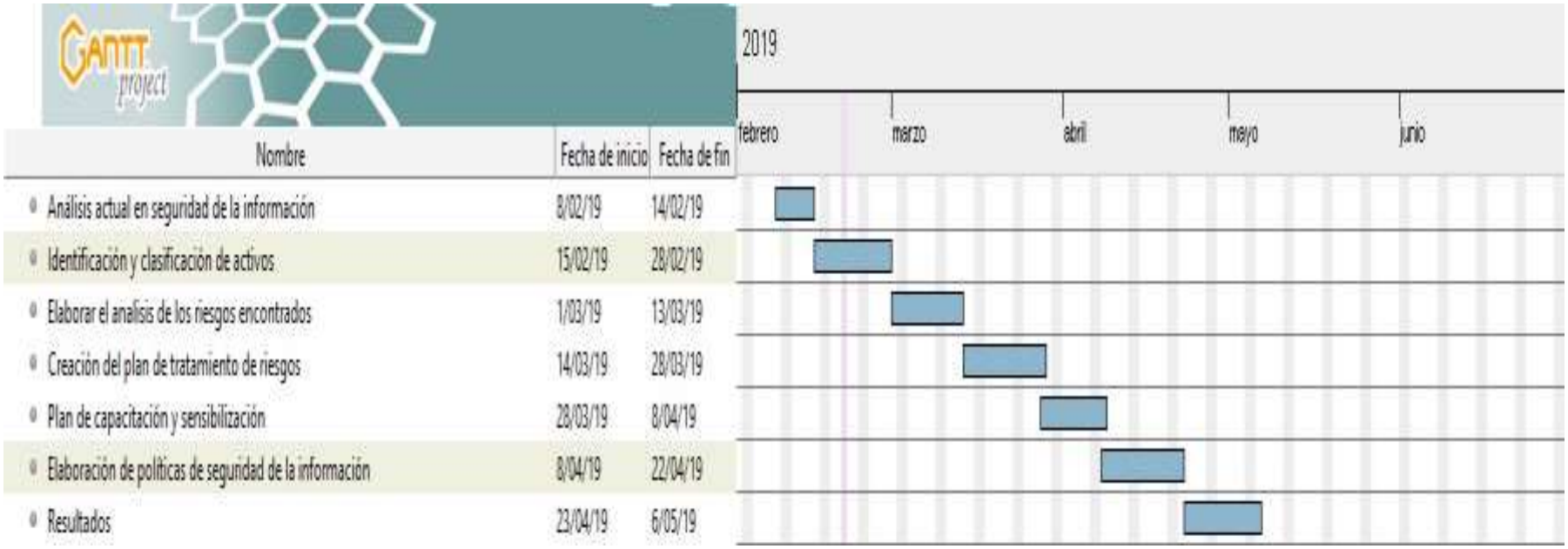
- Actualizar el manual de políticas de seguridad de la información cuando ocurran cambios significativos.

- Comprobar la eficacia de las mejoras incorporadas.

- Comunicar las mejoras realizadas a las máximas autoridades.

- Capacitar al personal que maneja la seguridad de la información, así como al personal técnico del área de Sistemas (administradores, desarrolladores, entre otros).

Gráfico Nro. 14: Diagrama de Gantt para el diseño de la propuesta.



Fuente: Elaboración Propia.

Tabla Nro. 31: Presupuesto del diseño de la propuesta.

Principales Rubros	**Acciones necesarias para lograr cada resultado**	**Unidad de Medida**	**Cantidad**	**Costo Unitario S/.**	**Costo Total a Precios de Mercado S/.**
Expediente Técnico		Estudio	1	2,500.00	2,500.00
Resultado 1: Clasificación de la Información existente	- Revisión de la información y documentación. - Identificación de riesgos. - Clasificación de la información existente. - Elaboración de políticas de seguridad de la información	Global	1	10,000.00	10,000.00
Supervisión		Global	1	2,000.00	2,000.00
Gastos Generales		Global	1	1,000.00	1,000.00
Total S/.					15,500.00

Fuente: Elaboración Propia.

VI. CONCLUSIONES

Teniendo en cuenta los resultados obtenidos en el presente trabajo de investigación, se concluye que la Municipalidad Distrital de Buena Vista Alta, la misma que permitirá mejorar los procesos de seguridad, confiabilidad y disponibilidad de la información. La interpretación realizada coincide con la hipótesis general a la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista alta – Casma; 2017, permitirá minimizar la pérdida de información, por lo tanto, concluyo diciendo que la hipótesis general es debidamente aceptada.

1. Para la propuesta de seguridad de información, se evaluó la situación actual de los procesos de seguridad tomando en cuenta la norma ISO 27001:2014 para la Municipalidad Distrital de Buena Vista Alta, permitiendo identificar los problemas de seguridad en la información.

2. Se demostró que la evaluación de los marcos de referencia permitió proponer mejoras en la seguridad de la información en la Municipalidad Distrital de Buena Vista Alta los cuales se refuerza con los resultados de la dimensión Necesidad de la propuesta de un sistema de la información con normas ISO 27001.

3. Se logró realizar la propuesta de la aplicación de la Norma ISO/IEC 27001, la cual mejora la seguridad de la información en las diversas áreas tecnológicas de la Municipalidad Distrital de Buena Vista Alta.

Como principal aporte es mejorar la seguridad de información y por ende impedir la pérdida y eliminación de información que le pertenecen a la Municipalidad Distrital de Buena Vista Alta.

El valor agregado es utilizar la norma ISO 27001 para verificar el nivel de seguridad de información de todas las áreas tecnológicas de la Municipalidad Distrital de Buena Vista Alta.

VII. RECOMENDACIONES

1. Es importante considerar que el Sistema de Gestión de Seguridad de la Información es un proceso de mejoramiento continuo, en donde los nuevos requerimientos de seguridad se ajusten a los cambios de la Municipalidad Distrital de Buena Vista Alta.

2. Evaluar periódicamente la seguridad de la información, utilizando las normas ISO 27001, en la Municipalidad Distrital de Buena Vista Alta. A fin de garantizar la aplicación de procesos preventivos que contribuyan a la

continuidad de los servicios y de este modo la Municipalidad se fortalezca en su reputación a través del uso de los sistemas de información.

3. Capacitación continua para el personal de TI en métodos y procesos de seguridad de la información y comunicación de la Municipalidad Distrital de Buena Vista Alta a fin de mejora sus competencias y actualización en nuevas metodologías y herramientas para la aplicación de la seguridad de la información.

4. La Unidad Técnica de Computación y Estadística, debe proponer la realización de la gestión para la Certificación de la norma ISO / IEC 27001, a fin de garantizar la implementación de acuerdo con las normas y protocolos establecidos por la empresa de certificación.

REFERENCIAS BIBLIOGRÁFICAS

1. Kosutic. Una guía para la pequeña empresa para la implementación de la iso 27001 con medios propios. Primera ed. Almeria: Advisera Expert Solutions Ltd; 2016.
2. Alemán Novoa CI. Metodología para la Implementación de un SGSI en la JDC: Aplicación de la norma ISO 27001 - SGSI en la Fundación Universitaria Juan de Castellanos de Tunja. Primera ed. España: Editorial Académica Española; 2017.
3. Guamán Seis JA. Diseño de un sistema de gestión de seguridad de la información para instituciones militares. Tesis. Quito: Politécnica Nacional, Ingenieria de Sistemas; 2015.
4. Bermúdez Molina G, Baión Sánchez. Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001 – sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros. Tesis. Guayaquil: Universidad Politécnica Salesiana Sede Guayaquil, Ingeniería de Sistemas; 2015.
5. Yugual Del Valle , Chilán Rodriguez. Análisis para la integración de un Sistema de Gestión de Seguridad de Información (SGSI) ISO-27001 Utilizando OSSIM para empresa Industrial. Tesis. Guayaquil: Universidad Politécnica de Salesiana Sede Guayaquil, Ingenieria de Sistemas; 2014.

6. Seclén Arana JA. Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001. Tesis de Grado. Lima: Universidad Nacional Mayor de San Marcos, Ingeniería de Sistemas e Informática; 2016.
7. Talavera Álvarez VR. Diseño de un Sistema de Gestión de Seguridad de la Información para una Entidad Estatal de Salud de acuerdo a la ISO/IEC 27001:2013. Tesis de Grado. Lima: Universidad Católica del Perú, Facultad de Ciencias e Ingeniería; 2015.
8. Aguirre Mollehuanca DA. Diseño de un Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A. Tesis de Grado. Tesis. Lima: Universidad Católica del Perú, Facultad de Ciencias e Ingeniería; 2014.
9. Castillo Collazos E. Sistema de Gestión de Seguridad de la Información en la Municipalidad Distrital de Pira aplicando la norma ISO/IEC 27001:2013. Tesis. Huaraz : Universidad Católica Los Ángeles de Chimbote, Ingenieria Sistemas; 2016.
10. Nizama Reyes. Evaluación de la seguridad para el personal informático y usuarios de sistemas en la Municipalidad Provincial de Piura. Tesis. Piura: Universidad Católica los Ángeles de Chimbote, Sistemas; 2015.
11. De la Cruz Alamo C. Mejora del programa de seguridad basada en el comportamiento del sistema integrado de gestión de prevención de riesgos y medio ambiente de GYM S.A. Tesis. Piura: Universidad de Piura, Ingeniería; 2014.
12. Pajito Mendoza H. Historial Municipal de Buena Vista Alta. Documento Municipal. Casma: Municipalidad Distrital, Municipalidad; 2018.
13. Landa Arroyo , Velazco Lozada. Constitución política del Perú 1993: sumillas, reformas constitucionales indice analitico. Novena ed. Landa Arroyo , Velazco Lozada , editors. Lima: Fondo; 2017.
14. Cucho Espinoza MA. Perú: Metodología para el diseño de una planificación estrategica interrelacionada con la Administración Presupuestaria en las entidades del sector público caso: "RENIEC". Tesina. Lima: Escuela de Administración de Negocios para Graduados , Lima; 2010.
15. Municipio al dia información confiable para la gestiòn. municipioaldia. [Online]. Lima; 2018 [cited 2018 Julio 30. Available from: https://municipioaldia.com/organizacion-municipal/.

16. Garcia Riega AJ. contraloria. [Online]. Lima; 2011 [cited 2018 Abril 04. Available from: https://apps.contraloria.gob.pe/transferenciagestion/material/Modulo_I/Organizaci%C3%B3n%20Municipal.doc.
17. Instituto Nacional de Estadistica e Información. INEI. [Online]. Lima; 2017 [cited 2018 Marzo 15 [Directorio Nacional de Municipalidades Provinciales, Distritales y de Centros Poblados 2015 Lima: Talleres de la Oficina de Impresiones del Instituto nacional de Estadística e Informática]. Available from: https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1420/index.html.
18. Perú top tours. perutoptours. [Online].; 2015 [cited 2018 Abril 04. Available from: http://www.perutoptours.com/index02ca_mapa_casma.html.
19. Mampis Mendoza. EL DISTRITO DE BUENAVISTA. [Online].; 2013 [cited 2018 julio 14. Available from: http://florconmaria.blogspot.com/2013/07/eldistrito-de-buenavista.html.
20. Alonzo de Arreaga SE. Seguridad de la Informacion. Tesis-Posgrado. Guatemala: Univercidad de San Carlos de Guatemala, Facultad de Ciencias Juridicas y Sociales; 2014.
21. Portal del Ministerio de Economía y Finanzas. MEF. [Online].; 2017 [cited 2018 Octubre 14 [Concepto de SIAF]. Available from: http://www.mef.gob.pe/index.php?option=com_content&view=article&id=2028&%20Itemid=101421.
22. Ministerio Economico y Finanzas. mef. [Online].; 2018 [cited 2018 Agosto 7 [Exposicion del Sistema Integrado de Gestión]. Available from: https://www.mef.gob.pe/es/.
23. Mef. Manuales del Sistema de Recaudación Tributaria Municipal (SRTM) - MEF. [Online].; 2018 [cited 2018 Octubre 16 [Inventario]. Available from: https://www.mef.gob.pe/es/rentas-catastro/manuales.
24. Vasconcelos Santillan J. Tecnologia de la Información. Segunda ed. Patria GE, editor. Mexico: Patria; 2015.
25. Gutiérrez González. Introducción a la Ingeniería. Primera ed. Marcombo , editor.

Madrid: Alfaomega; 2016.

26. Cubillos Ospina D. Tecnología De La Información Y Comunicación - Yopal. [Online].; 2012 [cited 2018 Nobiembre 11. Available from: https://sites.google.com/site/ticsyopal5/assignments/homeworkforweekofoctober 18th.
27. Arturo Betancourt S. Origen y evolución de las TIC y aportes a la educación. [Online].; 2012 [cited 2018 Abril 1. Available from: https://www.sutori.com/story/origen-y-evolucion-de-las-tic-y-aportes-a-laeducacion.
28. Villafuerte Quiroga D. solucionespracticas. [Online]. Lima; 2009 [cited 2018 marzo 1. Available from: https://solucionespracticas.org.pe/Descargar/398/3726.
29. Instituto Nacional de Calidad. INACAL. [Online].; 2016 [cited 2018 Octubre 30. Available from: https://www.inacal.gob.pe/principal/categoria/ntp.
30. Garre Gui S, Tortajada Gallego , Segovia Henares , Cruz Allende. Sistema de gestión de la seguridad de la información. Primera ed. España: Editorial UOC; 2018.
31. Vidalina De Freitas FN. Sistema de Gestion de Seguridad de La Informacion. Primera ed. Venezuela: Eae; 2012.
32. sbqconsultores. Consultora de Sistemas de Gestión y Normas ISO. [Online].; 2015 [cited 2018 Enero 27. Available from: https://www.sbqconsultores.es/el-ciclo-dedeming-o-circulo-pdca/.
33. Daltabuit Godas , Hernandez Audelo. La seguridad de la información. Primera ed. México: Limusa; 2007.
34. Harold F. Tipton MK. Information security management handbook. Sexto ed. Tipton HF, editor. Nueva york: Auerbach; 2008.
35. Cañizares Sales R, Merino Bada. Implantación de un sistema de gestión de seguridad de la información según ISO 27001. Primera ed. Español: FC Editorial; 2011.
36. Miguel Pérez C. Protección de datos y seguridad de la información. Cuarta ed. España: Ra-Ma ; 2015.
37. iso27000. Portal de ISO 27001 en español. [Online].; 2017 [cited 2017 Marzo 27. Available from: http://www.iso27000.es/iso27000.html.
38. Núñes Ponce J. JULIO NUNEZ DERECHO INFORMATICO. [Online].; 2016

[cited 2016 Marzo 1. Available from: http://julionunezderechoinformatico.blogspot.com/2016/01/.

39. elperuano. aprueban el uso obligatorio de la norma tecnica peruana NTP resolucion ministerial n° 004 2016 pcm. [Online].; 2016 [cited 2016 Enero 8. Available from: https://busquedas.elperuano.pe/normaslegales/aprueban-el-uso-obligatorio-de-lanorma-tecnica-peruana-ntp-resolucion-ministerial-no-004-2016-pcm-1333015-1/.
40. Rubio JA. isaca. [Online].; 2013 [cited 2013 Noviembre 11. Available from: http://www.isaca.org/chapters7/Madrid/Events/Documents/Principales%20Novedades%20de%20la%20ISO27001ISO%2027002%20-%20Paloma%20Garcia.pdf.
41. Sandoval Vargas C. Análisis de la norma ISO/IEC 27001. Diseño de Implementación en la red de una empresa. Tesis de Grado. Guayaquil: Universidad Católica de Santiago de Guayaquil, Sistema de Posgrado; 2014.
42. Namakforoosh M. Metodología de la investigación. Segunda ed. Mexico: Limusa; 2012.
43. Cauas D. Definicion de la Variables, enfoque y tipo de Investigacion. 2006. Articulo - Manual.
44. Hernandez Sampieri , Fernandez Collado , Baptista Lucio. Metodología de la investigación. Sexta ed. España: McGraw-Hill Interamericana; 2014.
45. Hernández Sampieri R, Fernández Collado C, Baptista Lucio P. Metodología de la investigación: Componentes de los Materiales de entrenamiento para Análisis de Corte Transversal. Primera ed. S.A PFeI, editor. Canada: MCGRAW-HILL; 1991.
46. Gómez. Introducción a la metodologia de la Investigación científica. Primera ed. Argentina: Editorial Brujas; 2006.
47. R. Peltier T. Fundamentos de seguridad de la información. Segunda ed. Publications A, editor. Guatemala: CRC PRESS; 2013.
48. definicionabc. Definición de Encuesta. [Online].; 2016 [cited 2017 abril 23. Available from: http://www.definicionabc.com/comunicacion/encuesta.php.
49. Muñoz Almendralejo TG. El Cuestionario como instrumento de investigación /evaluación. Tesis. España: Universitario Santa Ana, Sociologia; 2003.
50. Uladech. www.uladech.edu.pe. [Online].; 2019 [cited 2016 Enero 25. Available from:

https://www.uladech.edu.pe/images/stories/universidad/documentos/2016/codigode-etica-para-la-investigacion-v001.pdf.

ANEXOS

ANEXO NRO. 1: CRONOGRAMA DE ACTIVIDADES

CRONOGRAMA DE ACTIVIDADES					
N°	Actividades	Año 2019			
		Semestre II			
		1	2	3	4
1	Redacción del informe preliminar	X			
2	Revisión del informe final de la tesis por el Jurado de Investigación		X	X	

3	Aprobación del informe final de la tesis por el Jurado de Investigación			X	
4	Presentación de ponencia en jornadas de investigación				X
5	Redacción de artículo científico				X

Fuente: Elaboración Propia.

ANEXO NRO. 2: PRESUPUESTO

TITULO: Propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017.

ESTUDIANTE: Colonia Hernández Pedro Jesús.

INVERSIÓN: S/. 1.074.

FINANCIAMIENTO: Recursos propios.

Presupuesto desembolsable (Estudiante)			
Categoría	**Base**	**% o número**	**Total (S/.)**
Suministros (*)			
• Lapiceros	1.00	2	2.00
• Lápices	1.00	2	2.00
• Fotocopias	0.10	30 hojas	3.00
Servicios			
• Servicios de Internet	1.00	80hrs	80.00
• Uso de Turnitin	50.00	2	100.00
Sub total			187.00
Gastos de viaje			
• Pasajes para recolectar información	235.00		235.00
Sub total			235.00

Total, de presupuesto desembolsable			422
Presupuesto no desembolsable (Universidad)			
Categoría	**Base**	**% o número**	**Total (S/.)**
Servicios			
• Uso de Internet (Laboratorio de Aprendizaje Digital - LAD)	30.00	4	120.00
• Búsqueda de información en base de datos	35.00	2	70.00
• Soporte informático (Módulo de Investigación del ERP University - MOIC)	40.00	4	160.00
• Publicación de artículo en repositorio institucional	50.00	1	50.00
Sub total			400.00
Recurso humano			
• Asesoría personalizada (5 horas por semana)	63.00	4	252.00
Sub total			252.00
Total, de presupuesto no desembolsable			652.00
Total (S/.)			**1.074**

Fuente: Elaboración Propia.

ANEXO NRO. 3: CUESTIONARIO

TITULO: Propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017.

ESTUDIANTE: Colonia Hernández Pedro Jesús.

PRESENTACIÓN:

El presente instrumento forma parte del actual trabajo de investigación; por lo que se solicita su participación, respondiendo a cada pregunta de manera objetiva y veraz. La información a proporcionar es de carácter confidencial y reservado; y los resultados de la misma serán utilizados solo para efectos académicos y de investigación científica.

INSTRUCCIONES:

A continuación, se le presenta una lista de preguntas, agrupadas por dimensión, que se solicita se responda, marcando una sola alternativa con un aspa ("X") en el recuadro correspondiente (SI o NO) según considere su alternativa.

DIMENSIÓN 1: SATISFACCIÓN CON LA SEGURIDAD DE INFORMACIÓN ACTUAL.			
NRO.	**PREGUNTA**	**SI**	**NO**
1	¿Está de acuerdo con el servicio estable y orden de información para mayor seguridad en los sistemas de información?		
2	¿Usted cree que cumple con la práctica de estas políticas de seguridad para mayor énfasis en la información?		
3	¿Cree usted que las medidas del proceso de seguridad de la información son confiables para el acceso de la información?		
4	¿Usted tiene conocimiento sobre el uso de las herramientas de seguridad ante los softwares?		

5	¿Existen riesgos de perdida de datos en los recursos de información en la seguridad de los usuarios?		
6	¿Usted obtienen una buena protección física de sus equipos ante incidentes?		
7	¿Hay frecuencias de incidencias de fallos en la Municipalidad dañando los equipos de cómputo?		
8	¿Usted está satisfecho con el proceso de la gestión de una propuesta de seguridad de información?		
9	¿Usted cree que teniendo un control de medios de almacenamiento de datos resguardara la seguridad de información en la Municipalidad?		
10	¿Los sistemas de información permiten una gestión adecuada de los procesos de la Municipalidad?		

DIMENSIÓN 2: NECESIDAD DE LA PROPUESTA DE UN SISTEMA DE LA INFORMACIÓN CON NORMAS ISO 27001.			
NRO.	**PREGUNTA**	**SI**	**NO**
1	¿Cree usted que la capacitación le ayudara a tomar conciencia lo importante que es la seguridad de la información con Normal ISO 27001?		
2	¿Usted cree que la seguridad informática está desarrollada sin pensar originalmente en la protección de la información?		
3	¿Usted aprueba la gestión administrativa para el proceso de una buena gestión de seguridad de la información?		
4	¿Usted aprueba en la calidad de servicio para la mejor propuesta de las buenas prácticas?		
5	¿Cree usted que verificando su equipo de trabajo en la Municipalidad requiere de un monitoreo para determinar la falta de seguridad de información?		
6	¿Cree usted que la gestión de seguridad de la información confirme los reportes dados en situaciones importante de pérdidas totales de datos en la Municipalidad?		
7	¿Cree usted que el análisis de las divulgaciones ilícitas en la Municipalidad se tomara en cuenta la propuesta de la seguridad de la información?		
8	¿Usted tiene experiencia sobre instalaciones de programas ante las vulnerabilidades que ocasionan en los sistemas informáticos para la seguridad de la información?		
9	¿Usted cree que teniendo un control de medios de almacenamiento de datos resguardara la seguridad de información en la Municipalidad?		

10	¿Cree usted que la propuesta garantizara la mejora en los recursos de la seguridad de la información en la Municipalidad?		

Fuente: Elaboración Propia.