



**UNIVERSIDAD CATÓLICA LOS ÁNGELES
CHIMBOTE
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA
DE SISTEMAS**

**ANÁLISIS Y DISEÑO DE UN PLAN DE
SEGURIDAD INFORMÁTICA EN LA
MUNICIPALIDAD DISTRITAL DE CANCHAQUE –
PIURA; 2020.**

**TRABAJO DE INVESTIGACIÓN PARA OPTAR
EL GRADO ACADÉMICO DE BACHILLER EN
INGENIERÍA DE SISTEMAS**

AUTOR

**CUTIN ZAPATA, ALIPIO
ORCID: 0000-0002-1714-3089**

ASESOR

**MORE REAÑO, RICARDO EDWIN
ORCID: 0000-0002-6223-4246**

PIURA – PERÚ

2021

EQUIPO DE TRABAJO

AUTOR

CUTIN ZAPATA, ALIPIO
ORCID: 0000-0002-1714-3089

Universidad Católica Los Ángeles de Chimbote, Estudiante de Ingeniería
de Sistemas Pregrado, Piura, Perú

ASESOR

More Reaño, Ricardo Edwin
ORCID: 0000-0002-6223-4246

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

JURADO

Ocaña Velásquez Jesús Daniel
ORCID: 0000-0002-1671- 429X

Castro Curay José Alberto
ORCID: 0000-0003-0794-2968

Sullón Chinga Jennifer Denisse
ORCID: 0000-0003-4363-0590

HOJA DE FIRMA DEL JURADO Y ASESOR

DR. OCAÑA VELÁSQUEZ, JESÚS DANIEL
PRESIDENTE

MGTR. CASTRO CURAY, JOSÉ ALBERTO
MIEMBRO

MGTR. SULLÓN CHINGA, JENNIFER DENISSE
MIEMBRO

MGTR. MORE REAÑO, RICARDO EDWIN
ASESOR

DEDICATORIA

A mis padres, por brindarme todo el apoyo que necesitaba para realizar uno de mis sueños.

A mi hermano que siempre estuvo apoyándome a lo largo de mi carrera.

A mi docente que siempre me guio por el sendero educativo correcto.

Alipio Cutin Zapata

AGRADECIMIENTO

En primera instancia, agradezco a nuestro señor Dios, ya que nos brinda salud y energías suficientes para lograr el éxito.

A la universidad Católica los Ángeles de Chimbote quien fortalece nuestros conocimientos abundantemente para ser los mejores profesionales.

A los trabajadores de la Municipalidad Distrital de Canchaque por darme la oportunidad de investigar, indagar para mi trabajo de investigación.

A mis docentes asesores por la excelente enseñanza y dedicación al aprendizaje.

Alipio Cutin Zapata

RESUMEN

Esta tesis se encuentra bajo la línea de investigación de sistemas de gestión de la calidad y seguridad de la información, en la Municipalidad Distrital de Canchaque en el área de secretaria, fotocopiado y las 4 oficinas que cuentan con computadoras se puede analizar que los procesos de modificar información ya sea de los trabajadores como de los ciudadanos, es muy riesgoso porque cuenta con trabajadores que cambian cada cierto tiempo. además, como ya se sabe los trabajadores de escritorio con computadas están expuestos a el robo de información ya que cualquier otro trabajador que ingrese a su ordenador podría extraer o borrar información muy importante, ya sea también el mismo trabajador por error borre información que olvido guardar, el objetivo principal de esta investigación fue analizar y diseñar el plan de seguridad informática en la municipalidad distrital de Canchaque – para mejorar el control de datos e información esta. Esta investigación mantuvo el tipo de modelo cuantitativo a nivel de investigación descriptiva, el cual mantuvo el diseño no experimental de corte transversal. La investigación conto con una población de 10 trabajadores, la cual se tomó los 10 trabajadores en un estudio por conveniencia del investigador; En las técnicas se utilizaron la encuesta y la observación. Dándonos como resultado que el 90.00% de los trabajadores No están satisfechos con el sistema actual. La investigación dio por concluido analizando y diseñado un plan de seguridad informática dando resultados positivos con el nivel de aceptación de 100.00%, concluí exitosamente el objetivo general planteado.

Palabras clave: Municipalidad Distrital, Plan de seguridad y Seguridad Informática.

ABSTRACT

This thesis is under the research line of information security and quality management systems, in the District Municipality of Canchaque in the secretarial area, photocopying and the 4 offices that have computers, it can be analyzed that the processes of Modifying information, whether of workers or citizens, is very risky because it has workers who change from time to time. In addition, as you already know, desk workers with computers are exposed to the theft of information since any other worker who enters their computer could extract or delete very important information, either the same worker by mistake deletes information that he forgot to save, the main objective of this research was to analyze and design the computer security plan in the district municipality of Canchaque - to improve the control of data and information. This research maintained the type of quantitative model at the descriptive research level, which maintained the non-experimental cross-sectional design. The research had a population of 10 workers, which was taken by the 10 workers in a study for the convenience of the researcher; The techniques were used in the survey and observation. Giving us as a result that 90.00% of the workers are not satisfied with the current system. The investigation concluded by analyzing and designing a computer security plan giving positive results with the acceptance level of 100.00%, I successfully concluded the general objective set.

Keywords: District Municipality, Security Plan and Information Security.

CONTENIDO

EQUIPO DE TRABAJO	ii
HOJA DE FIRMA DEL JURADO Y ASESOR	iii
DEDICATORIA	iv
RESUMEN	vi
ABSTRACT.....	vii
CONTENIDO	viii
ÍNDICE DE GRAFICOS	vi
ÍNDICE DE TABLAS	vii
I. INTRODUCCIÓN	1
II. REVISIÓN DE LA LITERATURA	3
2.1 Antecedentes	3
2.1.1 Internacional	3
2.1.2 Nacional	5
2.1.3 Regional	7
2.2 Bases teóricas de la investigación	9
2.2.1 Municipalidad distrital de Canchaque – Huancabamba	9
2.2.2 Seguridad Informática.....	10
2.2.3 Las Tecnologías de información y comunicaciones (TIC).....	13
2.2.4 Base de datos	14
2.2.5 Sistemas de información	15
2.2.6 Windows Security	15
2.2.7 Seguridad de RED	15
2.2.8 Encriptación de Datos	16
2.2.9 Aspectos principales de seguridad informática	17
2.2.10 UML.....	17
2.2.11 Riesgos.....	18
2.2.12 Activos	19
2.2.13 Metodología Magerit	19
2.2.14 Norma ISO 27001	20
2.2.15 ISO 27001 al aplicar	21
III. HIPÓTESIS	23
IV. METODOLOGÍA.....	1
2.1 TIPO Y NIVEL DE LA INVESTIGACIÓN	1
2.2 DISEÑO DE LA INVESTIGACIÓN	1

2.3	UNIVERSO Y MUESTRA.....	2
2.4	DEFINICIÓN OPERACIONAL DE LAS VARIABLES EN ESTUDIO....	3
2.5	Técnicas e instrumentos de Recolección de Datos	5
2.6	Plan de Análisis.....	5
2.7	Matriz de Consistencia	6
2.8	Principios Éticos.....	8
V.	RESULTADOS	9
3.1	Resultados	9
3.2	Análisis de resultados.....	23
3.3	PROPUESTA DE MEJORA.....	24
3.3.1	Entorno Informático.....	24
3.3.2	Equipos Disponibles (Activos).....	24
3.3.3	Análisis	25
	Análisis de Procesos	25
	Clasificación de procesos.....	27
	Personal de acceso a PC:.....	27
	Vulnerabilidades	27
	Uso de Norma ISO 27001.....	28
	Diagnóstico	29
3.3.4	Diseño	30
	Nivel de seguridad informática	30
	Continuando con la ejecución, luego de haber realizado el cuestionario se procede a establecer las siguientes fases de seguridad informática en la municipalidad.	31
	Primera Fase:	31
	Segunda Fase:	32
	Tercera Fase:.....	33
	Cuarta Fase:	34
	Diagrama de Gantt	35
	Temas de charlas.....	36
	Porque aplicar este plan de seguridad	36
VI.	CONCLUSIONES	38
	RECOMENDACIONES.....	39
	REFERENCIAS BIBLIOGRÁFICAS.....	40
	Anexos	44
	Anexo 1: Cronograma de actividades	45
	Anexo 2: Presupuesto.	47
	Anexo 3: Cuestionario.	48

Anexo 4: Consentimiento informado	49
Anexo 5: Carta de aceptación.	50
Anexo 6: Validez de expertos.....	51
Anexo 6: Prueba piloto.....	54

ÍNDICE DE GRAFICOS

Gráfico Nro 1: Nivel de satisfacción respecto a la seguridad informática actual.....	14
Gráfico Nro 2: Resumen de la Dimensión Nivel de aceptación de la propuesta de mejora	20
Gráfico Nro 3: Resumen General de las Dimensiones	22
Gráfico Nro 4: Cronograma del Diseño del plan de seguridad informática	35

ÍNDICE DE TABLAS

Tabla Nro 1: Definición Operacional	3
Tabla Nro 2: Matriz de Consistencia	6
Tabla Nro 3: Nivel de satisfacción respecto a la seguridad Informática actual.....	9
Tabla Nro 4: Nivel de satisfacción respecto a la seguridad Informática actual.....	10
Tabla Nro 5: Nivel de satisfacción respecto a la seguridad Informática actual.....	11
Tabla Nro 6: Nivel de satisfacción respecto a la seguridad Informática actual.....	12
Tabla Nro 7: Nivel de satisfacción respecto a la seguridad Informática actual.....	13
Tabla Nro 8: Nivel de aceptación de la propuesta de mejora.	15
Tabla Nro 9: Nivel de aceptación de la propuesta de mejora.	16
Tabla Nro 10: Nivel de aceptación de la propuesta de mejora.	17
Tabla Nro 11: Nivel de aceptación de la propuesta de mejora.	18
Tabla Nro 12: Nivel de aceptación de la propuesta de mejora.	19
Tabla Nro 13: Resumen general de las dimensiones	21
Tabla Nro 14: Equipos tecnológicos.....	24
Fuente: elaboración propia.....	25

I. INTRODUCCIÓN

La seguridad de las Tecnologías de la Información y la seguridad de la información es un tema que preocupa cada vez más a organizaciones y administraciones públicas. Los últimos ciberataques han puesto en riesgo la seguridad de muchas empresas; las empresas se preocupan y valoran más la seguridad informática y la ciberseguridad para identificar y eliminar vulnerabilidad, protegerse contra intrusos, evitar que información confidencial, privilegiada y datos personales llegue a manos de otras personas ajenas a la organización y proteger los equipos físicos. Evitar pérdidas económicas y pérdidas de información es el objetivo (13).

En la municipalidad distrital de Canchaque se puede analizar que los procesos de extraer, copiar, borrar información ya sea de los trabajadores como de los ciudadanos que conforman dicho distrito, es muy riesgosos ya que cuenta con trabajadores que cambian cada cierto tiempo. Cuentan con 16 computadoras las cuales 10 trabajadores tienen acceso más de 1 PC, como ya se sabe los trabajadores de escritorio con Computadas están expuestos a el robo de información ya que cualquier otro trabajador que ingrese a su ordenador podría extraer o borrar información muy importante, ya sea también el mismo trabajador por error borre información que olvido de guardar.

Por este motivo, en la investigación se formula plantear una solución viable para el siguiente enunciado del problema ¿Analizar y diseñar un plan de seguridad informática en la municipalidad distrital de Canchaque – Piura para mejorar el control de datos e información la seguridad informática? La investigación se realizará en la municipalidad distrital de Canchaque - Piura; 2020. Siendo la investigación de tipo cuantitativa, nivel descriptivo, diseño no experimental de corte transversal.

Para esta investigación dada se planteó el objetivo general: Analizar y diseñar el plan de seguridad informática en la municipalidad distrital de Canchaque – para mejorar el control de datos e información. Se plantea los siguientes objetivos específicos:

1. Determinar el nivel de satisfacción respecto a la seguridad informática actual.
2. Realizar un análisis de la situación actual para para identificar las funciones del personal.
3. Diseñar una propuesta tecnológica para tener una mayor seguridad informática.

Se justifica tecnológicamente porque se le recomendó a la Municipalidad estar actualizada con las nuevas tecnologías, ya que esta mejora los servicios y seguridad y acelerara los procesos de ejecución al momento de realizar una operación o tramite, se justifica Operativamente porque esta propuesta de diseño y análisis mejorara la seguridad y actividades que se realizan u operan en la municipalidad distrital de Canchaque – Piura 2020; que actualmente en mi punto de vista son deficientes. Con esto lograremos una buena imagen para los ciudadanos y usuarios, se justifica económicamente ya que se necesita un análisis y diseño que ayude a mejorar la seguridad Informática de datos e información para que sus trabajadores y ciudadanos no tengan problemas al momento de realizar un tramiten y así pueden ahorrar tiempo y dinero.

Concluimos que con esta investigación lo más importante de analizar y diseñar un plan de seguridad informático fue centrarme más en las vulnerabilidades como los riesgos y amenazas, para dar la solución respectiva, ya que el 90% de los trabajadores sostenía que no estaban satisfechos con el sistema de seguridad informática actual mientras que el 10% sostenía que Si lo cual fue indispensable realizar este análisis y diseño de un plan de seguridad informático en la municipalidad distrital de Canchaque – Piura para mejorar el control de datos e información.

II. REVISIÓN DE LA LITERATURA

2.1 Antecedentes

2.1.1 Internacional

Según Noguera (36), en el año 2019 en su tesis titulada “Implementación de un sistema de detección de intrusos para venezolana del vidrio C.A”, el presente proyecto tiene como objetivo Implantar un sistema de detección de intrusos IDS en la empresa Venezolana del Vidrio C.A, y como objetivos específicos diagnosticar el estado de la infraestructura de seguridad informática de la organización, definir el IDS a utilizar en la implementación y configurar e integrar el IDS a la red de la organización. Se utilizo la siguiente metodología de investigación para el desarrollo del proyecto estuvo basada en la naturaleza del mismo, la cual está fundamentada en los criterios de la investigación tecnológica. Se concluye afirmando que el objetivo planteado se alcanzó de manera exitosa a través del desarrollo de las diferentes etapas las cuales van desde el levantamiento de informacional, capacidad de detectar ataques mientras sucede en tiempo real, así como de detenerlos inmediatamente o en cuestión de minutos, es el objetivo ideal. Desafortunadamente, muchas organizaciones actualmente no pueden detectar los ataques sino hasta días o incluso meses después de ocurridos.

Según CORREA, MENDOZA y MELENDEZ (1), en el año 2017 en su tesis titulada “Análisis y Diseño de un Sistema Para la Gestión de Archivos de la Oficina de Normalización Previsional”, el presente proyecto tiene como objetivo contar con un análisis y diseño de un Sistema, el cual implemente módulos, permitiendo manejar los procesos de Recepción, Envío, Atención de los Requerimientos de los Clientes y Devolución de documentos, esto a su vez va permitir manejar con mayor facilidad el proceso de otorgar pensiones y agilizar la evaluación de solicitudes y reducir tiempos de respuesta para atender mejor a los clientes internos. Para la ejecución del trabajo se usó las Metodologías: investigación

Aplicada, investigación Experimental y RUP. Para desarrollar la aplicación se hará uso del sistema gestor de base de datos MySQL, y se usará el lenguaje de programación PHP. Se concluyó que una de las mejores prácticas de la Ingeniería del Software, recomendable para cubrir necesidades y descubrir posibles debilidades de un proyecto en desarrollo, es la de mantener la documentación del mismo, desde el inicio del mismo y en cada una de las etapas, hasta su prototipo final; generando las entregas oportunas de los archivos entregables conforme al Cronograma del Proyecto.

Según Muñoz (31), en el año 2016 en su tesis titulada “Diseño de políticas de seguridad informática para la dirección de tecnologías de la información y comunicación (DTIC) de la universidad de cuenca”, el presente proyecto tiene como objetivo Analizar, diseñar políticas de seguridad Informática para la DTIC, en base a la Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27002:2009, manual de Políticas de Seguridad Informática-Mejores Prácticas Internacionales, y como objetivos específicos obtener información del personal que administra los diferentes sistemas informáticos, equipos de comunicación y computación, mediante visitas de campo, entrevistas, analizar el estado actual de la seguridad informática de las tres unidades que conforman la DTIC, y entregar a la DTIC un documento de políticas de seguridad informática en base de mejores prácticas. Se utilizó la siguiente metodología de investigación Experimental. Luego de haber obtenido, revisado y analizado la información relacionada con temas de seguridad informática que fue proporcionada por el personal que labora en las tres Unidades que conforman la DTIC, se pudo estimar que el porcentaje de cumplimiento inicial es del 52 % de acuerdo a los 11 dominios de seguridad de la norma ISO 27002, cabe indicar que existieron controles que su porcentaje de cumplimiento fueron del 0%, debido a la naturaleza de la Universidad; recordando que la norma ISO 27002 está diseñada para

cualquier tipo de entidad sea pública o privada, pequeña, mediana o grande.

2.1.2 Nacional

Según Ortiz, Ramos y Sullon (30), en el año 2020 en su tesis titulada “Análisis, diseño y elaboración de un prototipo para un sistema de administración y elección de rutas de transporte público”, el presente proyecto tiene como objetivo Realizar el análisis, diseño y elaboración de un prototipo para un sistema de administración y elección de rutas de transporte público urbano, y como objetivos específicos Obtener los requisitos funcionales de la aplicación que permita la administración y elección de transporte público, diseño de reportes y consultas de información útil para la gestión de las empresas de transporte. El método científico es un proceso destinado a explicar fenómenos, El nivel de la investigación es descriptiva correlacional, la tipología del proyecto es Básica/aplicativa, puesto que se ponen en práctica las herramientas de diseño de aplicaciones. Se concluye afirmando Desarrollado el prototipo para un sistema de administración y elección de rutas de transporte público urbano, se concluye que cumple con el objetivo, el prototipo cumple con la experiencia del usuario de acuerdo a las encuestas realizadas a los mismos, se refleja un 74,77 % de satisfacción al utilizar el prototipo.

Según Sánchez y Vargas (4), en el año 2018 en su tesis titulada “Análisis y diseño de edificios de concreto armado considerando la rigidez efectiva de sus elementos estructurales”, el presente proyecto tiene como objetivo Realizar el análisis y diseño de dos edificios de concreto armado evaluando los casos de elementos estructurales con rigidez de secciones agrietadas y no agrietadas para comparar su respuesta ante análisis sísmicos lineales y no lineales, y como objetivos específicos Realizar los análisis sísmicos de la norma E.030-2016 a los edificios de estudio considerando la rigidez de sus elementos según cuatro enfoques: Norma ACI, Norma ASCE, rigidez dependiente del refuerzo y secciones no agrietadas, diseñar los edificios analizados con la norma de diseño peruana E.060-2009.. investigación

Aplicada, investigación Experimental. Por lo que se concluye que el incremento de inseguridad acentúa cuando están constituidos principalmente por columnas. Asimismo, se concluye que en ninguno de los casos esta variación genera cambios en el diseño de elementos verticales.

Según Siancas (29), en el año 2016 en su tesis titulada “Análisis, diseño e implementación de un sistema de gestión del equipamiento hospitalario para el hospital universitario”, el presente proyecto tiene como objetivo Realizar el análisis, diseño e implementación de un Sistema de Información para el registro, seguimiento y control de los equipos hospitalarios y sus procesos de mantenimiento en el Hospital Universitario, y como objetivos específicos Identificar los procesos que se llevan a cabo dentro del Área de Estadística e Informática del Hospital Universitario, determinar los requerimientos funcionales y no funcionales del sistema basados en las necesidades de información de los usuarios.

investigación Aplicada, investigación Experimental. En conclusión, con la implementación y puesta en marcha del sistema, los procesos manuales relacionados con la gestión de equipos hospitalarios pasaron a automatizarse, como lo son: registro y administración de solicitudes de pedido y mantenimiento de equipos hospitalarios, registro y administración de órdenes de trabajo, programación de mantenimiento a los equipos e ingreso, asignación y administración de los mismos.

2.1.3 Regional

Según Mendoza (7), en el año 2019 en su tesis titulada “Sistema web de registro y búsqueda de incidencias en el área de soporte técnico para la Municipalidad Provincial de Piura”, el presente proyecto tiene como objetivo Desarrollar una aplicación web para la mejora del registro y búsqueda de incidencias en el área de soporte técnico de la Municipalidad Provincial de Piura y como objetivos específicos determinar cómo la aplicación web mejora el tiempo de registro de incidencias en la Municipalidad Provincial de Piura, determinar cómo la aplicación web mejora el tiempo de búsqueda de incidencias en la Municipalidad Provincial de Piura. El tipo de diseño de esta investigación realizada corresponde al diseño Cuasiexperimental, el diseño de la investigación realizada es de tipo descriptiva correlacional, debido a que en este caso se describió el proceso de registro de incidencias cuando se realizaba de manera manual hasta después del uso de la aplicación web para así determinar si se mejoró el proceso. Por lo tanto, se concluye que con el uso del sistema web se logró disminuir el tiempo de búsquedas de incidencias, se determinó que el porcentaje de incidencias atendidas sin el sistema web es de 69.60% y con el uso del sistema web se mejoró 95.15%. Por esta razón se concluye que con el sistema web se logró mejorar el porcentaje de incidencias atendidas.

Según Martínez F. (28), en el año 2017 en su tesis titulada “Análisis y diseño de un sistema de control de asistencia para la panificadora “pan de dios” –tumbes; 2017”, el presente proyecto tiene como objetivo Analizar y Diseñar un sistema de control de asistencia para mejorar los procesos de pago de la panadería “Pan de Dios”, Tumbes -2017, y como objetivos específicos Diagnosticar el proceso actual del control de la asistencia del personal de la panadería “Pan De Dios”, aplicar la metodología RUP para el diseño del sistema, Diseñar conceptual, lógica y físicamente la base de datos, diseñar el modelo de base de datos acorde con los requerimientos de la empresa, proponer un sistema de control de asistencia, para la

aprobación del proyecto por parte de la panificadora. El tipo de diseño de esta investigación realizada corresponde al diseño de investigación cuantitativa, experimental. En conclusión, El 80% del personal encuestado no está satisfecho con el registro de asistencia actual que se maneja en la panadería Pan de Dios ya que no hay un buen control de asistencias, no hay privacidad de información, hay problemas el proceso de pagos y se pierde mucho tiempo en el registro actual, el 93% de los trabajadores encuestados afirmaron que si es están de acuerdo con la satisfacción con propuesta de sistema de asistencia, ya que va a permitir automatizar procesos, logrando tener un buen control de la asistencia de los trabajadores de la panadería pan de dios.

Según Saavedra (8) en el año 2016 en su tesis titulada “Análisis y diseño de un sistema e-commerce para la gestión de ventas: caso empresa World of cakes”, el presente proyecto tiene como objetivo Producir y comercializar productos de repostería de alta calidad e innovación y como objetivos específicos elaborar productos que capten la atención de los posibles consumidores y que realicen la compra, elaborar los productos, de calidad e innovación, exquisito sabor y de menor costo, dar a conocer las ventajas que ofrece la materia prima de mejor calidad (frutas frescas y sin conservantes) que se utilizan con respecto a los productos elaborados con ésta, innovar con diseños creativos, sabores y productos que sean acordes a las preferencias de los clientes y a sus necesidades. El tipo de diseño de esta investigación realizada es experimental y de corte transversal. En conclusión, La propuesta de implementación de la tienda virtual, es rentable y beneficiosa para la empresa ya que el periodo de recuperación es de 2.7 meses, el valor actual neto es de 14 228.4 soles y la tasa interna de rentabilidad es de 51%. Con la implementación del sistema se tendrá un beneficio en el manejo de información de las ventas, además de estadísticas de ventas, clientes y productos actualizados en línea.

2.2 Bases teóricas de la investigación

2.2.1 Municipalidad distrital de Canchaque – Huancabamba

Reseña Histórica

Por medio de la ley número 2817, el seis de noviembre del año 1918, se estableció la capital llamada distrito del pueblo de Canchaque, sientio oficialmente hasta el día de hoy. Esta ley la promulgo José Pardo, gracias a las actividades y colaboraciones realizadas por Juan Ocaña, lo cual se agradece también al doctor Benjamín H. quien represento la institución de Huancabamba (provincia).

Ubicación

El distrito de Canchaque está ubicado en el NOR occidente del Perú. Piura – Huancabamba a 1200 metros sobre el nivel del mar, en 5 grados 22’-24’’ SUR (latitud) y en oeste a 79 grados, 36’-15’ del mediterráneo.

Objetivo Organizacional

Alcanzar resultados esperados en la visión, misión objetivos estratégicos y funcionales de su ámbito geográfico cumpliendo las políticas y normas.

Misión

Al 2020 Canchaque (municipalidad), se desenvuelve como una institución tecnológica, audaz y precisa que promueve el Desarrollo de sus pobladores, a si merando la calidad de vida, da servicios limpios en todo sentido de la palabra y su prioridad en el trabajo es la coordinación, cuenta con apoyo de cooperación(internacional-nacional), los cual nos permite tener un plan muy estratégico.

Visión

Nuestra visión es servir a nuestra propia población de Canchaque(distrito), con nuestro gobierno acogedor, que promovemos el Desarrollo de la población, para que pueda escuchar la voz de su gente para resolver sus problemas, comprometido con que sea capaz de escuchar las demandas de nuestra población, interactuando en sus problemáticas, fomentando la honradez, ser eficientes y promover la participación social.

2.2.2 Seguridad Informática

Los virus informáticos

Según Romero y otros autores (10), en su libro “INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES” Los principales y primordiales conceptos de la seguridad informática, son los virus informáticos, la PC(computadoras), lo único que les dan órdenes son los binarios (ceros y unos), hoy en día en las computadoras se plantean muchos conceptos e ideas ya sea el de crear, diseñar y programar apps, videojuegos entre otros se les conoce como software, ¿qué es el software?, se puede decir que su concepto es abstracto, ya que se le conoce como algo que no se puede tocar(intangible) es decir que son los que le dan órdenes a la computadora para realizar una acción determinada en un tiempo determinado.

Según Romero y otros autores (10), en su libro “INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES” Los procedimientos que son precavidos en la seguridad de la información (seguridad informática) casi ni se acuerdan de ello, puesto que piensan que solo nos hacen gastar tiempo, con las empresas pasa que ven esto como un gasto absurdo y no beneficioso por ejemplo, cuando pagamos un Seguro para nuestro vehículo y nunca hemos tenido un accidente pues sería como que hubiésemos pagado 20 años de

Seguro que nunca usamos pero ya sea el caso en un accidente pues este Seguro cubre todo con garantías.

El peligro de las copias de seguridad de los datos

Según Kevin y William (21), denominador común en la mayoría de nosotros es que, cuando queremos hacer una copia de seguridad, buscamos que sea de una forma que nos resulte cómoda. Si tenemos bastante espacio libre, lo copiamos todo. Y luego nos olvidamos. El número de copias de seguridad esparcidas por todos los rincones es enorme. Dejamos que se acumulen y nadie piensa en quitarlas hasta que se agota el espacio del servidor o del dispositivo de seguridad, "A menudo, las copias de seguridad contienen información vital y esencial, increíble en la que nadie piensa, sencillamente, porque es la copia de seguridad. No la protegen",

Según Kevin y William (21), Una empresa podía extremar la protección de algunos datos, pero las copias de seguridad de esos mismos datos se trataban como si carecieran de importancia. Cuando estuve fugitivo, trabajé para una firma legal que dejaba las cintas de las copias de seguridad en una caja a la puerta de la sala de ordenadores de acceso restringido para que una empresa de almacenamiento externo la guardara. Cualquiera habría podido robar las cintas con poco riesgo de que lo pillaran.) En COPIASEGURIDAD2, descubrió un área compartida en la que alguien había guardado la copia de seguridad de todos sus archivos más interesantes, de todo.

Proxy

Según Romero (34), en su libro titulado "Seguridad Informática y alta disponibilidad", Se denomina Proxy a todo equipo que ofrece un servicio de intermediario entre un equipo cliente y un equipo servidor. Es decir, el cliente hace una solicitud al equipo Proxy, y este se encarga de suplantarle y hacerla llegar al servidor. Este tipo de entorno suele ser muy habitual, ya

que nos permite filtrar las conexiones del cliente, forzar una autenticación, o directamente garantizar una determinada calidad de servicio.

Claves Simétricas y Asimétricas

Según Romero (34), en su libro titulado “Seguridad Informática y alta disponibilidad”, la seguridad no era algo que preocupara excesivamente a los primeros usuarios de las redes de comunicaciones. En efecto, usando éstas para poco más que enviarse correo electrónico y compartir alguna impresora dentro de una universidad u organización cerrada, pocos problemas de seguridad podrían producirse.

Tecnología defensiva en seguridad informática

Según Romero y otros autores (10), en su libro titulado “Introducción a la seguridad informática y el análisis de vulnerabilidades área de innovación y desarrollo”, cuando se habla de tecnología defensiva en el ámbito de la informática, lo primero que se suele venir a la cabeza compra de paquetes de antivirus, pero hay mucha más tecnología que puede complementar la seguridad de lo organización. Lo principal que se debe tener en cuenta es que la responsabilidad de la gestión de la parte tecnológica de la defensa de la infraestructura, ha de recaer sobre el departamento de IT o del centro de operaciones de seguridad, es posible y cada vez más habitual que existan departamentos de seguridad específicos en muchas organizaciones y parte de su labor va a ser coordinado con el trabajo del Departamento de IT, por lo que hay que tener precaución en la gestión administrativa.

Aquí la lista actualizada más utilizada, en seguridad informática por empresas y compañías (35):

- **Firewalls.** - Todas las compañías montan sistemas de filtrado de paquetes, bien mediante Firewalls. Existen FW personales cuya utilidad suele cuestionarse a favor de los IPS personales.
- **Antivirus.** -Se montan siempre a dos niveles: a nivel de red y a nivel de puesto de trabajo.

- **IDS.** -Los sistemas de detección de intrusos han estado ayudando a detectar problemas en las redes durante años, pero su incapacidad de detener los ataques que ellos mismos detectaban y la gran cantidad de alarmas que generaban han dado paso a los IPS
- **IPS.** -Están en pleno auge. Son capaces de detectar y detener tantos ataques conocidos como desconocidos, detectar y detener virus, troyanos, aislar hackers cuando se les detecta y hasta proteger a los otros elementos de seguridad de la red.
- **Control de acceso a red.** -Microsoft y Cisco están en plena pugna por “llevarse el gato al agua” en lo que a control de acceso a red se refiere y aunque recientemente anunciaron su intención de colaborar, lo cierto es que cada uno sigue por su lado.
- **VPN + PKI.** -Durante años el binomio VPN + PKI han dominado el mundo de los accesos remotos seguros pero la necesidad de instalar un cliente de VPN en el PC los ha hecho incómodos.
- **VPN + SSL.** -Sin más complejidad para el cliente que conectarse a una página web segura de la compañía para poder entrar en ella vía VPN.

2.2.3 Las Tecnologías de información y comunicaciones (TIC)

Según Andrada (11), en su libro “Nuevas Tecnologías de la Información y la Comunicación/NTICX”, Las Tecnologías de la Información y la Comunicación, a las cuales nos referimos de ahora en más como TIC, la que más confianza y respeto nos merece es la que desarrollaron dos investigadores de la Universidad de Manchester, Reino Unido, Europa: Richard Duncombe y Richard Heeks.

Según Andrada (11), en su libro “Nuevas Tecnologías de la Información y la Comunicación/NTICX”, Estos reconocidos expertos definieron a las TIC como los procesos y productos derivados de las nuevas tecnologías (hardware, software y canales de comunicación) relacionados con el almacenamiento, el procesamiento y la transmisión digitalizados de

información que permiten la adquisición, la producción, el tratamiento, la comunicación, el registro y la representación de la información en forma de voz, imágenes y datos.

Según Osorio (22), en su libro “Las tecnologías de la información y la comunicación” Las tecnologías de la información y la comunicación (TIC) -se afirma- pueden contribuir a tener avances significativos en muchos sectores, sin embargo, la evolución y adopción de las mismas planteará diferentes desafíos, ya que su empleo requiere nuevas habilidades y destrezas, por lo que todos los actores de estos espacios tendrán en algún momento que capacitarse en su uso, con todo lo que esto implica.

2.2.4 Base de datos

Según Catherine (12), en su libro “Base de datos” en el mundo de hoy las D.B. (bases de datos) se utilizan demasiado a tal punto que se puede buscar grupo e información de todo estilo y tamaño, para lo cual gigantes corporaciones gubernamentales, y pequeños hogares son encontrados por diferentes desarrolladores de potentes motores de búsqueda en las base de datos, ya que con frecuencia estas BD son muy utilizadas en forma directa o viceversa por ejemplo, cuando visita un portal de Internet el cliente que busca algún producto en específico, le muestran información acerca de lo que está disponible para ese entices su orden se almacena en una BD.

Según Catherine (12), en su libro “Base de datos” Incluso es supuesto para poder ver la información guardada de compras u órdenes anteriores que a haya realizado, entre todos los sitios web hay unos en particular que utilizan información de otros lugares donde el cliente ha obtenido o registrado datos de gustos o modelos de preferencia, las empresas tienden a aceptar la documentación de los pedidos e historial del supuesto cliente para luego brindar servicios cercanos a sus registros.

2.2.5 Sistemas de información

Según Hernández (13), en su investigación “LOS SISTEMAS DE INFORMACIÓN: EVOLUCIÓN Y DESARROLLO” El tener un fondo de competencia usando S.I. grandemente el trato acordado en el adecuado de recurso del S.I (sistema de información). Desarrollar un Sistema informático no es nada sencillo lo contrario resulta muy complicado desarrollarlo; el grupo u organizaciones que les llega nueva tecnología de la información sin tener ni idea que las necesidades de la empresa resolverán. Por lo tanto, es clave seguir los pasos de procedimiento para la documentación lo cual nos dice que temernos que saber que es Proyecto y cuál es la solución mediante implementar un sistema de información; es normal que se proporcione información para que se identifiquen los recursos de sistemas.

2.2.6 Windows Security

Según Tanenbaum (14), “Modern Operating Systems” Mantente actualizado y protegido. Al instalar las actualizaciones más recientes de Windows 10, obtendrás nuevas características y las mejoras de seguridad más recientes para que siempre estés protegido. Y lo mejor de todo: menos reinicios cuando más usas tu PC, simplemente establece tus horas activas.

2.2.7 Seguridad de RED

Según Molina (15), en su libro Titulado “Las Redes Locales”, Define una red de datos como una estructura formada por determinados medios físicos (dispositivos reales) y lógicos (programas de transmisión y control) desarrolla para satisfacer las necesidades de comunicación de una determinada zona geográfica. Se trata, pues, de un soporte que permite conexión de diversos equipos informáticos (o cualquier otro dispositivo electrónico) con el objetivo de suministrarles la posibilidad de que intercambien informaciones.

2.2.8 Encriptación de Datos

Mejorar seguridad de datos

Según Hernández (13), en su investigación “Los sistemas de información: evolución y desarrollo” por la información de la BD de una empresa, es un importante recurso de la corporación lo cual se debe dar restricción para evitar el mal uso de la información o datos; también se le protege de programas de terceros que intentan robar, borrar o manipular esta información sin ningún permiso. El procedimiento de una DB nos da restricciones de diferentes posiciones o niveles. Cuando alguien tiene acceso a una BD siempre es por BDMS es lo que al cliente o usuario le da niveles de seguridad para entrar o acceder a los datos ya sea contraseñas, pines entre otros; este es desarrollado para que ningún cliente o usuario tenga acceso ilegal, si por alguna razón entran sin autorización a los datos o intentan, estos se encriptan lo cual solo cuando el verdadero usuario entra estos datos se desencriptan en el BDMS. Para el usuario puede que no sea de su conocimiento los datos encriptados, en particular a cada usuario se le visualiza solo una vista predeterminada. Por ejemplo, en una institución, en las oficinas de admisión solo se les da acceso a una parte de la información del personal que opera en la institución.

Según Hernández (13), en su investigación “Los sistemas de información: evolución y desarrollo” en la visualización de los ítems de la BD, ya sea solo actualización de los registros o agregar nuevos. Si por alguna razón un usuario intenta acceder a sin autorización, si ID será copiado a ABD y los datos del BDMS será encriptados instantáneamente lo cual es de mucho beneficio para la empresa u organización que vela por cuidar su integridad de BD e información.

2.2.9 Aspectos principales de seguridad informática

Según Romero (10), en su libro “Introducción a la seguridad informática y el análisis de vulnerabilidades” Indica que una política de mesas limpias y bufete escampado debidamente implantado, eludiría que se produzcan accesos no autorizados a la información, la educación de los empleados debe remeter aspectos relacionados con el uso del Mailing, en este sentido es destacado trasladarles cómo identificar un correo fraudulento y qué hacer ante esta situación para evadir los ataques de phishing. Cada vez es más regular que los empleados usen las redes sociales, especialmente aquellas que tienen índole gremial, por el contrario, se debe puntualizar e implantar una legislatura de uso válido para proteger la fama online.

2.2.10 UML

Rumbaugh, Jacobson y Booch (16), en su libro “El Lenguaje Unificado De Modelado” La enseñanza y experiencia práctica necesaria para analizar una preocupación y proyectar una alternativa, centrándose en el uso oportuno de las tecnologías orientadas a objetos y el manejo de los pasos simplificados en el desarrollo de proceso de aplicaciones. Es la tesis clave y se realizan discusiones en tropel, yuxtapuesto con actividades guiadas por el profesor para presentar una ayudante básica y costumbre de observación y diseño OOAD que chancleta desde la colección de requisitos hasta el diseño del sistema. Los alumnos aprenderán las ventajas de aprovechar el lenguaje de modelado descriptivo UML usando un utensilio, que les aprobará comunicar los conceptos y decisiones, entender la inquietud y una alternativa proposición, al igual que ocasionar los diagramas y documentación que describen el problema y la posibilidad.

¿Qué es UML?

Según Fowler y Kendall (23), en su libro “UML gota a gota” el lenguaje unificado de modelado o UML es el sucesor de la oleada de métodos de análisis y diseño orientados a objetos que surgió a finales de la de cada de

los 1980 y principios de la siguiente. El UML unifica, sobre todo, los métodos de booch, Rumbaugh y Jacibson, pero su alcance llegará a ser mucho más Amplio. En estos momentos el UML está en pleno proceso de estandarización con el OMG y estoy Seguro de que se convertirá en el lenguaje de modelado estándar del futuro.

¿Porque analizar y diseñar con UML?

Según Fowler y Kendall (23), en su libro “UML gota a gota” En resumidas cuentas, la cuestión fundamental del Desarrollo del software es la escritura del Código. Después de todo, los diagramas son solo imágenes bonitas. Ningún usuario va a agradecer la belleza de los dibujos; lo que el usuario quiere es software que funcione. Por lo tanto, cuando esté considerando usar UML, es importante preguntarse por qué lo hará y cómo le ayudara a usted cuando llegue el momento de escribir el Código. NO exista una evidencia empírica adecuada que muestre si estas técnicas son buenas o malas, pero en las siguientes subsecciones analizaré las razones que con frecuencia encuentro para justificar su uso.

2.2.11 Riesgos

Los pequeños negocios no están exentos de riesgos laborales siendo esta característica en cuanto a su dimensión un riesgo ya en sí, debido por ejemplo al tamaño de los locales. Es importante seguir unos procedimientos de trabajo seguros con tareas tan básicas como el orden y la limpieza, mantenimiento de los materiales de trabajo, entre otros, disponer de una señalización que nos ayude a trabajar más seguros es posible si introducimos en el negocio señales de prohibición, advertencia, entre otros (37).

2.2.12 Activos

Se define el Activo de una empresa como el conjunto de bienes, derechos y otros recursos de los que es propietaria una compañía, por ejemplo, muebles, oficinas, equipos informáticos, también se incluyen aquellos de los que esperamos tener un beneficio futuro (38).

2.2.13 Metodología Magerit

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados (25):

- Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
- Decidir a qué amenazas están expuestos aquellos activos.
- Resolver qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Fijar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Modificación de la calificación de seguridad de servicios o datos (25):

- Típicamente requiere la modificación de un sistema ya operativo. Raramente implica el desarrollo de un nuevo sistema o la desaparición de partes actualmente operativas.
- La iniciativa la lleva el responsable de seguridad, actuando el responsable de sistemas como subsidiario.

2.2.14 Norma ISO 27001

La mejora de las empresas se consigue aprendiendo o auto enseñándose de los incidentes de seguridad de la empresa, los problemas identificados en las auditorías como también, los problemas de rendimiento y, además, las quejas de las partes interesadas y por ultimo las ideas que se generan al momento de las supervisiones por la dirección (40).

Para cada caso identificada, se deberá registrar la siguiente lista (40):

- Lo que ocurrió.
- Si el evento tuvo consecuencias indeseables, qué acciones se tomaron para controlarlo y mitigarlo.
- La causa raíz del evento (si se determina).
- La acción tomada para eliminar la causa raíz (si es necesario).
- La evaluación de la efectividad de cualquier acción tomada

Un SGSI no es solo de requerir su implementación sino se refiere al mantenimiento y mejora de las medidas de seguridad, por ello que la norma ISO 27001 nos brinda la solución de mejora siendo continua con la evaluación de los activos y riesgos con el objetivo general de la protección y defensa de los mismos, ISO 27001 es un sistema que tiene un enfoque basado en el ciclo de mejora continua o de Deming. Dicho ciclo consiste como ya sabemos, en Planificar-Hacer- Verificar Actuar, por lo que se le conoce también como ciclo PDCA (40).

2.2.15 ISO 27001 al aplicar

En relación o referencia con la seguridad de la información hay normas allegadas o ligadas a la misma, pero la norma ISO 27001 es factor principal con similitud a las demás, ya esta norma implementa un SGSI certificable en cuando se refiere a la seguridad de los activos de información. Generalmente se eligen las áreas más críticas o vulnerables en materia de gestión de la información. Luego de definido el alcance, se debe formular y divulgar una política de la gestión de la seguridad de la información que establezca los lineamientos generales que la organización tendrá que en cuenta los riesgos de la información, considerando los requisitos legales propios de la empresa (41).

El eje central de la planificación del SGSI consiste en fijarse e identificar o analizar los riesgos de la información, en relación o coordinación con las posibles amenazas y los puntos centrales vulnerables de la organización en cuanto se refiere a la confiabilidad, disponibilidad y seguridad de la información (41).

A partir de la identificación de aquellos riesgos, y sobre su análisis de valoración, se definirán exactamente los planes de control o tratamiento de riesgo. Incluyendo la documentación y la aplicación de los procedimientos o procesos necesarios tales como los controles, así como la formación y la concienciación de los laboradores o trabajadores respecto a la seguridad de la información (41).

La verificación y observación incluye la medición del desempeño que ofrece el SGSI, la eficacia de los controles y la evaluación, revisión de los riesgos implementados, la recisión del mismo por parte de la dirección y la realización de auditorías internas al sistema (41).

Áreas o Dominios de Seguridad de la ISO/IEC 27001 (41):

- A 5: Políticas de seguridad de la Información.

- A 6: Organización de la seguridad de la información.
- A 7: Seguridad de los Recursos Humanos.
- A 8: Gestión de recursos.
- A 9: Control de Acceso.
- A 10: Criptografía.
- A 11: Seguridad física y ambiental.
- A 12: Seguridad Operacional.
- A 13: Seguridad de las Comunicaciones.
- A 14: Adquisición, desarrollo y mantenimiento de Sistemas.
- A 15: Relaciones con los proveedores.
- A 16: Gestión de Incidentes en Seguridad de la Información.
- A 17: Aspectos de Seguridad de la Información para la gestión de la continuidad del negocio.
- Anexo 18: Cumplimiento.

III. HIPÓTESIS

EL ANÁLISIS Y DISEÑO DE UN PLAN DE SEGURIDAD INFORMÁTICA EN LA MUNICIPALIDAD DISTRITAL DE CANCHAQUE – PIURA MEJORARÁ EL CONTROL DE DATOS E INFORMACIÓN.

Hipótesis específicas

1. La encuesta desarrollada determinara la satisfacción de la seguridad actual en la municipalidad.
2. Realizar un análisis de la situación actual identificara las funciones del personal.
3. Diseñar una propuesta tecnológica nos dará una mayor seguridad informática.

IV. METODOLOGÍA

2.1 TIPO Y NIVEL DE LA INVESTIGACIÓN

Es tipo cuantitativo de nivel descriptiva, Sáez (18), se utiliza para describir las características de una población, situación o fenómeno. No trata de responder las causas de los fenómenos, no puede describir lo que causó una situación, por tanto, no se puede utilizar como base de una relación causal donde una variable afecta a otra. Por eso motivo tiene bajo requerimiento de la validez interna (18).

Fernández y Días (17), la investigación cuantitativa es aquella en la que se recogen y analizan datos cuantitativos sobre variables. La investigación cuantitativa trata de determinar la fuerza de asociación o correlación entre variables, la generalización y objetivación de los resultados a través de una muestra para hacer inferencia a una población de la cual toda muestra procede. Tras el estudio de la asociación o correlación pretende, a su vez, hacer inferencia causal que explique por qué las cosas suceden o no de una forma determinada (17).

Esta Investigación tiene un enfoque cualitativo ya que se requiere la recolección de la información para tener un análisis completo de la actual situación de la empresa y el tipo de la investigación es descriptiva.

2.2 DISEÑO DE LA INVESTIGACIÓN

Hernández R. Fernández C., Baptista M.P. (19), en su investigación “. Metodología De La Investigación. V”, Diseño no experimental, de corte transversal, de una sola casilla. No experimental por su dimensión temporal o el número de momentos o puntos en el tiempo, en los cuales se recolectan datos. Los diseños de investigación transaccional o transversal recolectan datos en un solo momento, en un tiempo único. Su propósito es describir variables y analizar su incidencia e interrelación en un momento dado (19).

2.3 UNIVERSO Y MUESTRA

Hernández R. y otros (32), el Universo es la población total del trabajo que estamos desarrollando, por lo que se dice que el universo es el todo del sector que vamos a trabajar, muy diferente a la muestra y entonces una vez que se obtiene o se sabe con certeza el tamaño del universo ya se puede tomar la muestra.

Pazmiño (20), En efecto, la muestra constituye un subgrupo representativo del universo y esta representatividad sugiere -como ya hemos dicho que la muestra mantenga las características esenciales del universo; y, el que posteriormente podamos extender los resultados obtenidos por el estudio de la muestra a todo el universo, implica que los elementos de la fracción deban seleccionarse de manera aleatoria, es decir, al azar, a fin de garantizar que todos los elementos tengan la misma posibilidad de ser escogidos.

Mi universo consta de 10 trabajadores y como muestra fue por intención o juicio de 10 trabajadores.

2.4 DEFINICIÓN OPERACIONAL DE LAS VARIABLES EN ESTUDIO

Tabla Nro 1: Definición Operacional

Variable	Definición conceptual	Dimensiones	Indicadores	Definición Operacional
ANÁLISIS Y DISEÑO DE UN PLAN DE SEGURIDAD INFORMÁTICA	La seguridad de sus grupos de PC y otros dispositivos dispersos pueden tener una mayor seguridad de administrar, recuperar, procesar, almacenar y distribuir su información.	Nivel de satisfacción respecto a la seguridad informática actual	-Administración -Recuperar información -Dispositivos de PC -Procesos -Análisis	Se utilizo un cuestionario de 10 preguntas dividido en 2 dimensiones, en las cuales los trabajadores de la municipalidad responderán: SI=1 NO=0
		Nivel de aceptación de la propuesta de mejora	-Seguridad actual -Modificar o borrar datos -Clientes y trabajadores satisfechos -Mejor la seguridad informática	

			-Aprobación trabajadores	de	
--	--	--	-----------------------------	----	--

Fuente: Elaboración propia

2.5 Técnicas e instrumentos de Recolección de Datos

El concepto de técnicas de recogida de información engloba todos los medios técnicos que se utilizan para registrar las observaciones o facilitar el tratamiento. Dentro de la expresión “medios técnicos” están inmersos, por una parte, los instrumentos objetos con entidad independiente y externa y los recursos medios utilizados para obtener y registrar la información. Por ejemplo, utilizando como técnica el cuestionario, podemos manejar como instrumento un cuestionario cerrado, empleando como recurso el ordenador.

Para este trabajo de investigación eh tenido conveniente utilizar la técnica de encuesta y el instrumento de recolección de datos fue un cuestionario de 10 preguntas las cuales 5 están referidas a mi primera dimensión y las otras 5 a mi segunda dimensión.

2.6 Plan de Análisis

Eh analizado el por qué a veces los procesos de tramite no son seguros informáticamente, también analice cuales son los principales tramites y los organice, realice una encuesta de 10 preguntas a 10 trabajadores los cuales tienen acceso a la manipulación de datos eh información, mis preguntas fueron validadas por 3 expertos y están anexadas en anexos, una vez terminada mi encuesta proseguí a tabular los datos para un mayor orden de datos, utilice el software de Excel para tabular mis encuestas luego de eso analice los datos obtenidos y diseñe una propuesta de mejora la cual la municipalidad obtuvo una mejor atención a los pobladores y trabajadores de este distrito.

2.7 Matriz de Consistencia

Tabla Nro 2: Matriz de Consistencia

Problema	Objetivos	Hipótesis	Metodología
<p>¿Analizar y diseñar un plan de seguridad informática en la municipalidad distrital de Canchaque – Piura mejora el control de datos e información?</p>	<p>OBJETIVO GENERAL</p> <p>Realizar el plan de seguridad informática en la municipalidad distrital de Canchaque – para mejorar el control de datos e información.</p> <p>Objetivos específicos</p> <p>Con la finalidad de poder lograr el objetivo general, se establecieron los siguientes objetivos específicos:</p>	<p>El análisis y diseño de un plan de seguridad informática en la Municipalidad distrital de Canchaque – Piura mejorará el control de datos e información.</p> <p>Hipótesis específicas</p> <ol style="list-style-type: none"> 1. La encuesta desarrollada determinara la satisfacción de la seguridad actual en la municipalidad. 2. Realizar un análisis de la situación actual identificara las funciones del personal. 	<p>Tipo: Cuantitativo</p> <p>Nivel: Descriptiva</p> <p>Diseño: No experimental de corte trasversal.</p> <p>Universo: 10 personas Muestra: 10 personas</p>

	<ol style="list-style-type: none"> 1. Determinar el nivel de satisfacción respecto a la seguridad informática actual. 2. Realizar un análisis de la situación actual para identificar las funciones del personal. 3. Diseñar una propuesta tecnológica para tener una mayor seguridad informática. 	<ol style="list-style-type: none"> 3. Diseñar una propuesta tecnológica nos dará una mayor seguridad informática. 	
--	---	--	--

Fuente: Elaboración propia.

2.8 Principios Éticos

Durante el desarrollo de la presente investigación denominada “ANÁLISIS Y DISEÑO DE UN PLAN DE SEGURIDAD INFORMÁTICA EN LA MUNICIPALIDAD DISTRITAL DE CANCHAQUE – PIURA; 2020.”. Han tenido en cuenta el código de ética para la investigación, versión 002 del 2019, el cual tiene por finalidad establecer los principios y valores éticos, de lo cual se ha tenido en cuenta la protección a la persona implica resguardar si privacidad, confidencialidad, religión, entre otros. Libre participación y derecho a estar informado que es básicamente que mis participantes en mi proyecto de investigación estén completamente informados y más que todo salvaguardar los derechos de autor. Beneficencia y no-maleficencia está agrupando con este proyecto porque este principio ético esta como base el no causar ningún daño y en lo contrario causar efectos positivos que se multipliquen. Justicia es clave para este proyecto de investigación por eso es muy relevante que todo este trabajo de investigación trate por igualdad y con justicia a mis participantes desde varios puntos de vista y por último eh integrado a mis principios éticos la integridad científica para garantizar u asegurar claridad en el transcurso de mi proyecto de investigación, incluyendo análisis, comunicación de resultados y desarrollo para todo lo implicado en el desarrollo de mi investigación (39).

V. RESULTADOS

3.1 Resultados

Primera Dimensión: Nivel de satisfacción respecto a la seguridad Informática actual.

Tabla Nro 3: Nivel de satisfacción respecto a la seguridad Informática actual.

Frecuencias de distribución y respuestas allegadas al Nivel de satisfacción respecto a la seguridad Informática actual. sobre, el Análisis y diseño de un plan de seguridad informática en la municipalidad distrital de Canchaque – Piura; 2020.

Alternativa	n	%
Si	1	10.00
No	9	90.00
Total	10	100.00

Fuente: Cuestionario aplicado a los trabajadores del Municipalidad Distrital de Canchaque, respecto a la pregunta ¿Existe en dicha Municipalidad un responsable del área de la seguridad informática?

Aplicado por: Cutin A, 2020.

En la **Tabla Nro 3**, se observa que el 90.00% de los trabajadores sostienen que, No hay un responsable en el área de la seguridad informática en dicha municipalidad, y el 10.00% dice que Si hay un responsable en el área de la seguridad informática.

Tabla Nro 4: Nivel de satisfacción respecto a la seguridad Informática actual.

Frecuencias de distribución y respuestas allegadas al Nivel de satisfacción respecto a la seguridad Informática actual. Sobre, el Análisis y diseño de un plan de seguridad informática en la municipalidad distrital de Canchaque – Piura; 2020.

Alternativa	n	%
Si	4	40.00
No	6	60.00
Total	10	100.00

Fuente: Cuestionario aplicado a los trabajadores del Municipalidad Distrital de Canchaque, respecto a la pregunta ¿Ha ocurrido algún incidente de seguridad informática en su puesto de trabajo en el último año?

Aplicado por: Cutin A, 2020.

En la **Tabla Nro 4**, se observa que el 60.00% de los trabajadores sostienen que, No ha ocurrido un incidente de seguridad informática en su puesto de trabajo dicha municipalidad, y el 40.00% dice que Si ha ocurrido ningún incidente de seguridad informática en su puesto de trabajo.

Tabla Nro 5: Nivel de satisfacción respecto a la seguridad Informática actual.

Frecuencias de distribución y respuestas allegadas al Nivel de satisfacción respecto a la seguridad Informática actual. Sobre, el Análisis y diseño de un plan de seguridad informática en la municipalidad distrital de Canchaque – Piura; 2020.

Alternativa	n	%
Si	10	100.00
No	00	-
Total	10	100.00

Fuente: Cuestionario aplicado a los trabajadores del Municipalidad Distrital de Canchaque, respecto a la pregunta ¿Cree que el sistema de gestión basado en la ISO 27001 ayudara en la seguridad de información en la Municipalidad de Canchaque?

Aplicado por: Cutin A, 2020.

En la **Tabla Nro 5**, se observa que el 100.00% de los trabajadores sostienen el sistema de gestión basado en la ISO 27001 Si ayuda a en la seguridad de información en dicha municipalidad.

Tabla Nro 6: Nivel de satisfacción respecto a la seguridad Informática actual.

Frecuencias de distribución y respuestas allegadas al Nivel de satisfacción respecto a la seguridad Informática actual. Sobre, el Análisis y diseño de un plan de seguridad informática en la municipalidad distrital de Canchaque – Piura; 2020.

Alternativa	n	%
Si	10	100.00
No	00	-
Total	10	100.00

Fuente: Cuestionario aplicado a los trabajadores del Municipalidad Distrital de Canchaque, respecto a la pregunta ¿Cree Usted que una charla como esta sea de mucha importancia?

Aplicado por: Cutin A, 2020.

En la **Tabla Nro 6**, se observa que el 100.00% de los trabajadores sostienen que Si, es de mucha importancia una charla sobre el tema de seguridad informática.

Tabla Nro 7: Nivel de satisfacción respecto a la seguridad Informática actual.

Frecuencias de distribución y respuestas allegadas al Nivel de satisfacción respecto a la seguridad Informática actual. Sobre, el Análisis y diseño de un plan de seguridad informática en la municipalidad distrital de Canchaque – Piura; 2020.

Alternativa	n	%
Si	09	90.00
No	01	10.00
Total	10	100.00

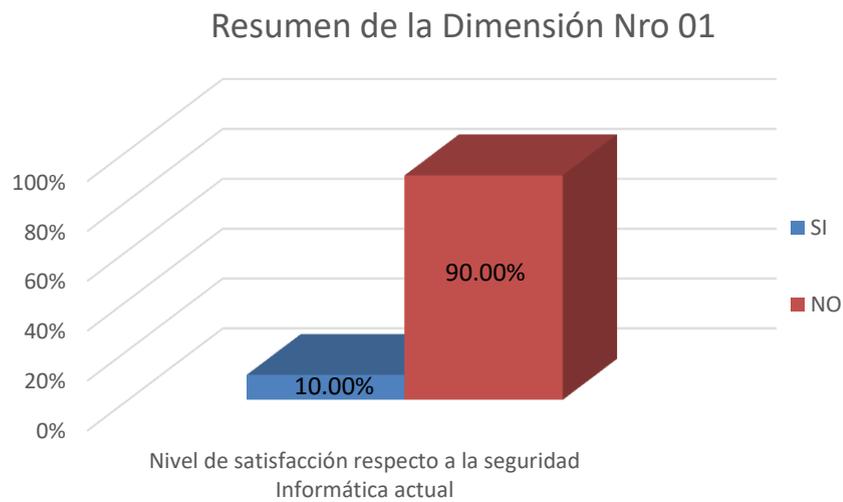
Fuente: Cuestionario aplicado a los trabajadores del Municipalidad Distrital de Canchaque, respecto a la pregunta ¿Cree que es necesario aplicar controles de seguridad para evitar robo o daño de información importante para la Municipalidad Distrital de Canchaque?

Aplicado por: Cutin A, 2020.

En la **Tabla Nro 7**, se observa que el 90.00% de los trabajadores sostienen que Si, es necesario aplicar controles de seguridad de información en dicha Municipalidad y el 10.00% sostiene que No es necesario aplicar controles de seguridad de información en dicha Municipalidad.

Gráfico Nro 1: Nivel de satisfacción respecto a la seguridad informática actual

Distribución de frecuencias y respuestas relacionada al Nivel de satisfacción respecto a la seguridad Informática actual. sobre, el Análisis y diseño de un plan de seguridad informática en la municipalidad distrital de Canchaque – Piura; 2020.



Fuente: Cuestionario aplicado a los trabajadores del Municipalidad Distrital de Canchaque.

Segunda Dimensión: Nivel de aceptación de la propuesta de mejora

Tabla Nro 8: Nivel de aceptación de la propuesta de mejora.

Frecuencias de distribución y respuestas allegadas al Nivel de aceptación de la propuesta de mejora, sobre, el Análisis y diseño de un plan de seguridad informática en la municipalidad distrital de Canchaque – Piura; 2020.

Alternativa	n	%
Si	2	20.00
No	8	80.00
Total	10	100.00

Fuente: Cuestionario aplicado a los trabajadores del Municipalidad Distrital de Canchaque, respecto a la pregunta ¿Conoce Usted sobre el tema de seguridad informática?

Aplicado por: Cutin A, 2020.

En la **Tabla Nro 8**, se observa que el 80.00% de los trabajadores sostiene que, No conocen sobre el tema de seguridad informática, mientras que el 20.00% SI conoce sobre el tema.

Tabla Nro 9: Nivel de aceptación de la propuesta de mejora.

Frecuencias de distribución y respuestas allegadas al Nivel de aceptación de la propuesta de mejora sobre, el Análisis y diseño de un plan de seguridad informática en la municipalidad distrital de Canchaque – Piura; 2020.

Alternativa	n	%
Si	10	100.00
No	00	-
Total	10	100.00

Fuente: Cuestionario aplicado a los trabajadores del Municipalidad Distrital de Canchaque, respecto a la pregunta ¿Considera que la seguridad de información debe ser vital en la Municipalidad?

Aplicado por: Cutin A, 2020.

En la **Tabla Nro 9**, se observa que el 100.00% de los trabajadores sostiene que, Si es importante que la seguridad de información debe ser vital en la Municipalidad.

Tabla Nro 10: Nivel de aceptación de la propuesta de mejora.

Frecuencias de distribución y respuestas allegadas al Nivel de aceptación de la propuesta de mejora sobre, el Análisis y diseño de un plan de seguridad informática en la municipalidad distrital de Canchaque – Piura; 2020.

Alternativa	n	%
Si	00	--
No	10	100.00
Total	10	100.00

Fuente: Cuestionario aplicado a los trabajadores del Municipalidad Distrital de Canchaque, respecto a la pregunta ¿Considera que la Municipalidad le da importancia suficiente a la seguridad informática?

Aplicado por: Cutin A, 2020.

En la **Tabla Nro 10**, se observa que el 100.00% de los trabajadores sostiene que, No le dan la importancia suficiente al tema de la seguridad informática en dicha municipalidad.

Tabla Nro 11: Nivel de aceptación de la propuesta de mejora.

Frecuencias de distribución y respuestas allegadas al Nivel de aceptación de la propuesta de mejora sobre, el Análisis y diseño de un plan de seguridad informática en la municipalidad distrital de Canchaque – Piura; 2020.

Alternativa	n	%
Si	3	30.00
No	7	70.00
Total	10	100.00

Fuente: Cuestionario aplicado a los trabajadores del Municipalidad Distrital de Canchaque, respecto a la pregunta ¿Conoce Usted sobre la norma ISO 27001 en la seguridad de información?

Aplicado por: Cutin A, 2020.

En la **Tabla Nro 11**, se observa que el 70.00% de los trabajadores sostiene que, No conoce sobre la norma ISO 27001 en la seguridad de información y el 30.00% Si conoce.

Tabla Nro 12: Nivel de aceptación de la propuesta de mejora.

Frecuencias de distribución y respuestas allegadas al Nivel de aceptación de la propuesta de mejora sobre, el Análisis y diseño de un plan de seguridad informática en la municipalidad distrital de Canchaque – Piura; 2020.

Alternativa	n	%
Si	01	10.00
No	09	90.00
Total	10	100.00

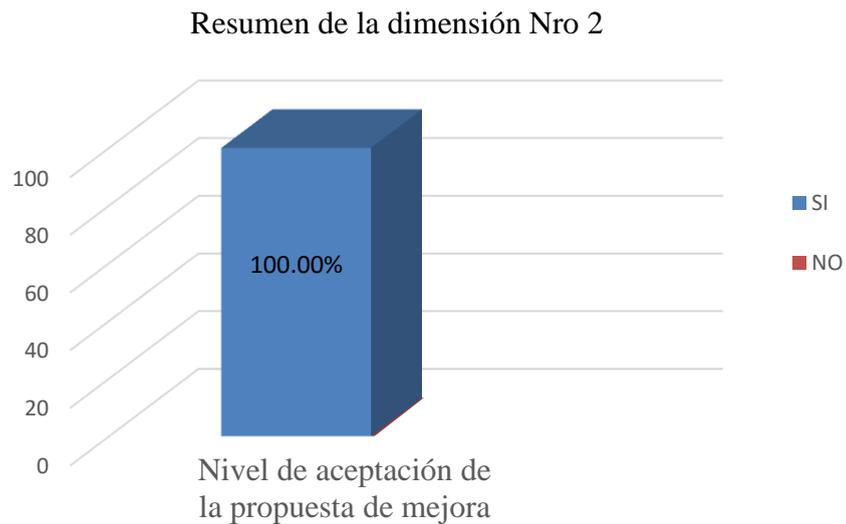
Fuente: Cuestionario aplicado a los trabajadores del Municipalidad Distrital de Canchaque, respecto a la pregunta ¿La Municipalidad imparte constantemente capacitaciones de seguridad Informática y la norma ISO 27001?

Aplicado por: Cutin A, 2020.

En la **Tabla Nro 12**, se observa que el 90.00% de los trabajadores sostiene que, No Imparten capacitaciones de seguridad Informática y la norma ISO 27001 y el 10.00% dice que Si imparten capacitaciones.

Gráfico Nro 2: Resumen de la Dimensión Nivel de aceptación de la propuesta de mejora

Distribución de frecuencias y respuestas relacionada al Nivel de aceptación de la propuesta de mejora sobre, el Análisis y diseño de un plan de seguridad informática en la municipalidad distrital de Canchaque – Piura; 2020.



Fuente: Cuestionario aplicado a los trabajadores del Municipalidad Distrital de Canchaque.

RESUMEN GENERAL DE LAS DIMENSIONES

Tabla Nro 13: Resumen general de las dimensiones

Resumen general de dimensiones, en relación al ANÁLISIS Y DISEÑO DE UN PLAN DE SEGURIDAD INFORMÁTICA EN LA MUNICIPALIDAD DISTRITAL DE CANCHAQUE – PIURA; 2020.

		Si		No		Total	
		n	%	n	%	n	%
Nivel de satisfacción respecto a la seguridad informática actual		01	10.00	09	90.00	10	100.00
Nivel de aceptación de la propuesta de mejora		10	100.00	-	-	10	100.00

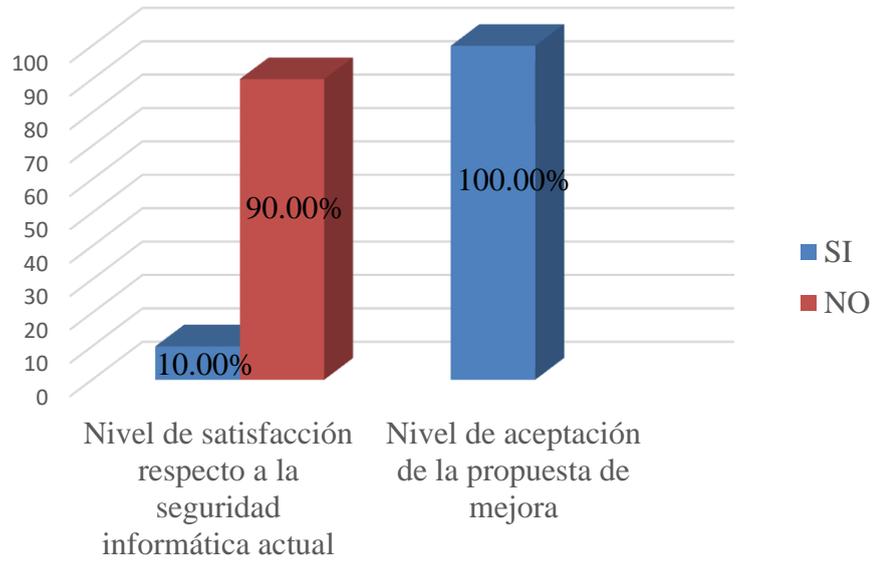
Fuente: Cuestionario aplicado a los trabajadores de la municipalidad Distrital de Canchaque – Piura; 2020.

Aplicado por: Cutin A, 2020.

En la Tabla Nro 13, se observa que el 90% de los trabajadores sostienen que No, es necesario aplicar controles de seguridad de información en dicha Municipalidad y el 10% sostiene que Si, a su vez el 100% de los trabajadores sostiene que, SI es importante que la seguridad de información debe ser vital en la Municipalidad.

Gráfico Nro 3: Resumen General de las Dimensiones

Resumen general de dimensiones, en respecto al Análisis y diseño de un plan de seguridad informática en la municipalidad distrital de Canchaque – Piura; 2020.



Fuente: Cuestionario aplicado a los trabajadores de la municipalidad Distrital de Canchaque – Piura; 2020.

3.2 Análisis de resultados

El actual proyecto tiene como propósito el objetivo general: Analizar y diseñar el plan de seguridad informática en la municipalidad distrital de Canchaque – para mejorar el control de datos e información.

1. Según el objetivo, Los resultados obtenidos en la dimensión 1 sobre el Nivel de satisfacción respecto a la seguridad informática actual, se observa que el 90% de los trabajadores No están satisfechos respecto a la seguridad actual, mientras el 10% afirma que Si, estos datos al ser comparados con lo encontrado por Martínez F. (28), en su tesis titulada “Análisis y diseño de un sistema de control de asistencia para la panificadora “pan de dios” – tumbes; 2017”, el cual obtuvo resultados beneficiosos, el 93% de los trabajadores encuestados afirmaron que si es están de acuerdo con la satisfacción con propuesta de sistema de asistencia. Con estos resultados se confirma que Analizar y diseñar el plan de seguridad informática en la municipalidad distrital de Canchaque si es necesario de aplicar, además MAGERIT (25), en su libro nos dice que el uso de tecnologías de la información y comunicaciones (TIC) supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que gestiones que prudentemente debes romance con medidas de seguridad que sustenten la confianza de los usuarios de los servicios.
2. Al respecto de la dimensión número 2: Nivel de aceptación de la propuesta de mejora, los resultados obtenidos son del 100% de los trabajadores los cuales aceptan la propuesta de mejora, lo cual podemos comparar con el resultado de la investigación de Correa A. J., Mendoza R. A., Meléndez J. I. (1), el cual redacta en el año 2017 su tesis titulada “Análisis y Diseño de un Sistema Para la Gestión de Archivos de la Oficina de Normalización Previsional” diseñaron el sistema de información al 100% por la aceptación que tenían sobre su análisis lo cual permita mejorar los flujos de trabajo en la Coordinación de Archivos y su interacción con las demás divisiones de la Institución.

3.3 PROPUESTA DE MEJORA

Esta propuesta de mejora está desarrollada bajo la metodología MAGERIT, basado con la NORMA ISO 27001 específicamente para hacer cumplimiento las normas dentro de un laboratorio de trabajo tecnológico y he tenido conveniente fijarme en los riesgos de información, Este plan se divide en 4 fases principales, que más adelante las encontrarán.

3.3.1 Entorno Informático

La municipalidad distrital de Canchaque cuenta con 10 oficinas las cuales se realizan diversos trámites a la población y a sus trabajadores mismos, aquí la lista específica y concreta de las diez oficinas:

- Oficina de secretaria
- Oficina de tramites documentarios
- Oficina de fotocopiado e impresiones
- Oficina de administración
- Oficina de digitalización de documentos
- Oficina de Registros
- Oficina de RENIEC
- Oficinas de recursos humanos
- Oficina de asistencia Administrativa
- Oficina de Soporte técnico

3.3.2 Equipos Disponibles (Activos)

Tabla Nro 14: Equipos tecnológicos

Nro.	Nombre de oficina	Equipos
1	Oficina de secretaria	2 PC y 1 impresora
2	Oficina de tramites documentarios	2 PC y 1 impresoras

3	Oficina de fotocopiado e impresiones	2 PC y 2 fotocopiadoras
4	Oficina de administración	3 PC
5	Oficina de digitalización de documentos	1 PC 1 fotocopiadora
6	Oficina de Registros	1 PC
7	Oficina de RENIEC	2 PC 1 fotocopiadoras
8	Oficinas de recursos humanos	1 PC
9	Oficina de asistencia Administrativa	1 PC
10	Oficina de Soporte técnico	1 PC

Fuente: elaboración propia

En total la Municipalidad cuenta con 16 ordenadores, 4 fotocopiadoras y 2 impresoras repartidas en las diferentes oficinas ya mencionadas.

3.3.3 Análisis

Análisis de Procesos

En la municipalidad distrital de Canchaque analice y estudie los procesos que se ejecutaban a diario, aquí dejo los procesos relacionados con la manipulación y adquisición referida a la informática o el parque tecnológico de la municipalidad:

- Archivar casos: cualquier documento mal fundado o no terminado, su siguiente paso es ser archivado físicamente; si es de grado de

importancia mayor es escaneado y guardado en la computadora de la oficina de secretaria.

- Recepción de Solicitudes: Cuando una solicitud llega a la municipalidad es anexada u registrada con una copia la cual se llama cargo y todas las solicitudes se guardan físicamente y en el disco duro de la secretaria.
- Recepción de Actas: una vez decepcionada un acta, su proceso es realizar un documento de su validez y almacenarlo en su disco duro de la PC.
- Solicitar partida de nacimiento: cuando un ciudadano solicita un acta de nacimiento se procede a registrar los datos del solicitante en un disco duro para luego sea procesada.
- Actualización de Portal Web: La información de la municipalidad debe estar actualizada en el portal web de la municipalidad, y supervisión de dicho portal no se da acabo, el cual no está actualizado.
- Impresión de documentos: los documentos son enviados en la nube o llevados físicamente en USB (Pen Drive).

Clasificación de procesos

Los procesos ya mencionados están referidos al ámbito tecnológico, el cual son las computadoras, impresoras, fotocopadoras, utilización de Pendrive (USB) entre otros, lo cual están agrupados por procesos:

- Recursos municipales, son utilizados por la participación de los ciudadanos como los trabajadores.
- Acción municipal, las acciones que se toman luego de que se solicitan los recursos municipales.
- Gastos municipales, el gasto implicado y su importancia en los presupuestos participativos, que son documentos de suma importancia donde llegan los datos fijos del presupuesto destinado a la municipalidad de Canchaque y son revisados por el alcalde, el gerente, una persona contable entre otros.

Personal de acceso a PC:

- Alcalde
- Administrador
- Secretarias
- Contable
- Soporte técnico

Vulnerabilidades

- Software sin licencia
- No usar Usuarios
- Uso inadecuado de USB
- El no conocimiento de la Norma ISO 27001
- No hay protocolos establecidos por si hay una incidencia

Uso de Norma ISO 27001

La municipalidad no cumple con el uso de la norma ISO 27001, por ello no es beneficiada con las siguientes mejoras:

- Implantar políticas de seguridad, en las compras, disposición y uso de las TI en la Municipalidad Distrital de Canchaque.
- El gerente y el alcalde deben presentar obligación de innovar productos o servicios tecnológicos que concuerden con los procesos de la Municipalidad Distrital de Canchaque.
- Implantar una serie de procedimientos que velen por la Seguridad informática dando respaldo a la información y datos en la Municipalidad Distrital de Canchaque.
- Implantar procesos que fijen la fiabilidad de los datos e información en la Municipalidad Distrital de Canchaque.
- Establecer los procedimientos de la documentación para el anexo del inventario de tecnología TI en la Municipalidad Distrital de Canchaque.
- Establecer las responsabilidades y roles del personal encargado de TI en la Municipalidad Distrital de Canchaque.
- Dejar en claro los roles de los USERS que hacen uso de los equipos tecnológicos en base a sus funciones en la Municipalidad Distrital de Canchaque.
- Brindar charlas o capacitaciones al personal que labora en el uso de los equipos tecnológicos de la Municipalidad Distrital de Canchaque.
- Establecer las políticas de sanciones por uso inadecuado o alguna falta indebida en la información o TI.
- Establecer los ambientes óptimos para la infraestructura TI de la Municipalidad Distrital de Canchaque.
- Establecer los procesos de solicitudes en cuanto refiere a al servicio al usuario o servicio al soporte TI de la Municipalidad Distrital de Canchaque.

Diagnóstico

El diagnóstico que puedo dar es de que la municipalidad tiene una infraestructura muy pobre en el tema de seguridad informática lo cual está expuesta posibles ataques de phishing, Robo de información, entre otros llegando afectar no solo a la misma municipalidad sino también a los trabajadores y ciudadanos.

Además, la municipalidad no imparte capacitaciones de seguridad informática, como también, no hace uso adecuado de la norma ISO 27001 por lo que no se le atribuye una serie de mejoras, como Innovación de productos o servicios tecnológicos, datos e información fiable, entre otras. Sus equipos son manipulados por mas de una persona, siendo esto una desventaja clara para el avance tecnológico de la municipalidad de Canchaque; su sitio web no esta actualizado por lo que si intentamos acceder este no nos permitiría, la municipalidad tiene una deficiencia clara en los accesos al personal de las computadoras, siendo por aquí que se maneja la nueva información y documentación, lo cual la hace de alto riesgo, su cableado se encuentra en buenas condiciones, como la seguridad de sus equipos de Internet esto es un punto a favor de la y concluyo el 90% de los trabajadores que laboran con computadoras en la municipalidad no están satisfechos con su seguridad informática actual, además el 100% si desea un plan de seguridad informática en la municipalidad.

3.3.4 Diseño

Nivel de seguridad informática

Para plan de ejecución es necesario primero medir el grado de seguridad informática por lo cual se debe aplicar el siguiente cuestionario con toda la veracidad posible:

El siguiente cuestionario está desarrollado hacia el encargado de soporte técnico con el fin de ver el estado de seguridad de información en la Municipalidad distrital de Canchaque.			
	Pregunta	SI	NO
1	¿La municipalidad invierte presupuesto en ciberseguridad?		
2	¿Los trabajadores de la municipalidad tienen la formación que necesitan para prevenir errores de seguridad informática?		
3	¿Los trabajadores de la municipalidad son capaces de identificar un virus/malware?		
4	¿Conoces las aplicaciones y dispositivos extraíbles que utilizan en la municipalidad?		
5	¿Gestionas el uso seguro de redes sociales y correo electrónico?		
6	¿Controlas los datos empresariales de la municipalidad?		
7	¿Los trabajadores de la municipalidad hacen un uso adecuado de las contraseñas y datos personales?		
8	¿Los trabajadores de la municipalidad conocen los riesgos de uso de redes wifi públicas?		
9	¿Controlas la seguridad de todos los usuarios de la municipalidad?		
10	¿Cuentas con un plan de prevención de riesgos informáticos?		

Fuente: elaboración propia

Continuando con la ejecución, luego de haber realizado el cuestionario se procede a establecer las siguientes fases de seguridad informática en la municipalidad.

Primera Fase:

Como primera fase iniciamos en la gestión de S.I. (seguridad informática), donde se implantan responsabilidades, procedimientos, roles y estándares referidos a la gestión de seguridad informática.

- Fijar verbalmente y por escrito al responsable del Área de seguridad informática.
- Fijar y definir los roles y misión del responsable Seguridad Informática.
- Fijar la delegación encargada de las gestiones de la seguridad informática.
- Crear un documento de incidencias donde se anexen todos los casos sobre seguridad informática para que futuras autoridades se fijen en los casos registrados en la municipalidad distrital de Canchaque.
- Fijar cada uno de los procedimientos de seguridad para el uso de la infraestructura T.I.
- Establecer quienes son únicos dueños de los archivos de cada una de las PC de la municipalidad.
- Crear una lista publica donde se visualice la infraestructura TI para que los trabajadores y pobladores que conforman la municipalidad estén al tanto de estos equipos y software.
- Contratar un asesor para poner la toma de decisiones para la aplicación de este plan de seguridad informática.

Segunda Fase:

Como segunda fase estamos viendo la implantación de control de seguridad de la fase 1, esto es para disminuir el riesgo de seguridad informática actual, en otras palabras, la segunda fase esta referida a la ejecución de la norma ISO 27001.

- Brindar capacitaciones a los laboradores y ciudadanos de la municipalidad sobre la seguridad informática y como se practica la norma ISO 27001, en dicha municipalidad y temas referidos al buen uso de infraestructura TI.
- Aplicar o poner en marcha las inspecciones de seguridad sobre la seguridad actual que tiene la municipalidad y fijándose en la integridad lógica u física de la información.
- Fijar y limitar las políticas y roles sobre la gerencia de pasos de los sistemas de información.
- Uniformar Usuarios, esto ara que los laboradores de la municipalidad distrital de Canchaque tengan personalmente un usuario y contraseña para cada PC.
- Fijar y definir normas para el correcto uso de la información eh archivos de las computadoras y así logren tener la importancia necesaria dicha información de la municipalidad distrital e Canchaque.
- Fijar procedimientos que nos den a saber las obligaciones y roles de los laboradores, pasantes, ciudadanos, estudiantes (practicante) hacia la seguridad informática.
- Verificar el correcto y apropiado uso de las TIC para así crear nuevos métodos de uso a estas tecnologías.
- Limitar los procesos de las gestiones con los cambios que son necesario modificar en los aplicativos de la municipalidad distrital de Canchaque.

- No excluir esta seguridad informática en las gestiones de negocios de o tratados que se suelen dar en la municipalidad distrital de Canchaque.
- Registrar y analizar todas las faltas cometidas sobre seguridad informática.
- Observar la potencia y beneficios de implementar cámaras de seguridad o sistemas que detecten algún inicio de incendio.
- Establecer BackUp a los funcionarios que cumplan un rol crítico dentro de las actividades que se ejecutan en el área de sistemas.

Tercera Fase:

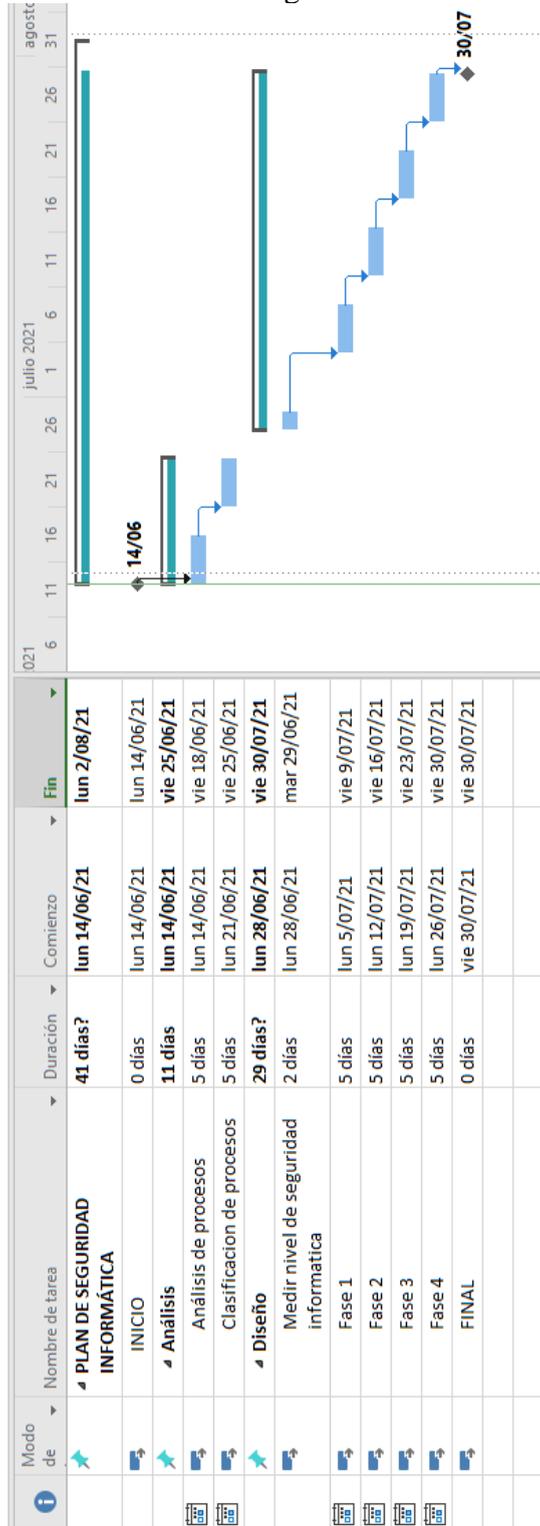
- Gestionar el monitoreo de la seguridad informática, comprobando su eficiencia con el fin de realizar ajustes a este diseño de plan de seguridad informática.
- Gestionar los monitoreos constantes para prevenir algún tipo de problemas con la seguridad de la información.
- Ver el alcance de realizar compras de software u herramientas para verificar los correos electrónicos, mensajes, documentos tengan algún archivo malicioso, entre otros.
- Ejecutar las gestiones de seguridad sin antes haberlas diseñado.
- Verificar si se está cumpliendo con las gestiones de correcto uso de activos.
- Verificar los accesos, la correcta utilización de la red y la comunicación.
- Verificar si los servidores de la página Web están operando de forma normal ya que son servicios contratados.
- Verificar si se está cumpliendo con los protocolos establecidos de seguridad de Data-Center.
- Guardar los resultados de las verificaciones o inspecciones que se han realizado.

Cuarta Fase:

- Una vez fijados los puntos deficientes con respecto la seguridad informática se procede a mejorar esos aspectos con un determinado plan.
- Aplicar los protocolos de seguridad a la página web de la municipalidad distrital de Canchaque.
- Una vez identificadas las mejoras se procede a incorporarlas en las gestiones de seguridad informática.
- Siempre que haya cambios drásticos en la infraestructura TI actualizar el reglamento de normas de seguridad informática.
- Verificar la eficiencia de las nuevas mejoras realizadas respecto a la seguridad informática.
- Siempre poner en conocimiento al alcalde, personal que labore en esta área si se realiza algún cambio para bien o para mal en este aspecto de la seguridad informática.
- Realizar capacitaciones abiertas y libre para la población, trabajadores incluyendo al alcalde y especialmente a los encargados del área de sistemas.

Diagrama de Gantt

Gráfico Nro 4: Cronograma del Diseño del plan de seguridad informática



Fuente: elaboración propia

Concluyendo las 4 fases de este plan de seguridad informática, aquí le dejamos algunas recomendaciones muy puntuales para que cuando estas cuatro hayan culminado su ejecución, tengan estos Tips

Temas de charlas

Como es imprescindible en estas cuatro fases aplicar charlas a los trabajadores y ciudadanos que conforman la municipalidad distrital de Canchaque se sugiere abordar temas generales como los siguientes, pero no confundiendo o alejándose de las charlas sobre los problemas principales de seguridad informática en dicha municipalidad:

- Que es un Plan de seguridad informática.
- Importancia de seguridad Informática en empresas.
- Recomendaciones para tener un sistema de seguridad informática.
- Como actuar en caso de un posible incidente referido a la seguridad informática o un CIBERATAQUE

Porque aplicar este plan de seguridad

Con la coyuntura que se está viviendo sobre delitos informáticos que se están propagando generalizando a gran magnitud y escala. Cada día más es indiscutible que una municipalidad distrital de Canchaque cuente con un plan de seguridad informática ya que, antes que pueda ocurrir un incidente o problema con este tema de protección a la información, tenemos que estar prevenidos para evitar dichos inconvenientes en la municipalidad y así en futuras gobernaciones los ciberataques o mala manipulación de la información de los trabajadores como de los clientes, la municipalidad quedaría inmersa a tener serios problemas los cuales pueden llegar a afectar la ISO 27001 y los distintos sectores regionales y nacionales los cuales están comprometidos en información de la municipalidad distrital de Canchaque.

Si una municipalidad quiere sobresalir y ser reconocida debe ser competente a las necesidades de hoy en día, tiene que contar con sistemas de TIC actualizados y con gran grado de alta disponibilidad para los trabajadores y ciudadanos, esto implica en tema general tener un plan de que abarca muchos temas relacionados a la coyuntura de la actualidad.

VI. CONCLUSIONES

Por los resultados obtenidos son de un 100% de satisfacción por parte de los trabajadores, el cual responde al objetivo general Analizar y diseñar el plan de seguridad informática en la municipalidad distrital de Canchaque – para mejorar el control de datos e información, se ha concluido con éxito el análisis lo cual me fue más importante centrarme en las vulnerabilidades como los accesos inapropiados y los procesos mal ejecutados, además concluyó que diseñe un plan de mejora para dar la solución y que la municipalidad tenga a su disposición un plan de seguridad informático, por lo cual su información y datos estarán protegidos.

1. EL 90.00% de los trabajadores de la Municipalidad de Canchaque manifiestan que no están satisfechos con respecto a la seguridad informática actual, pues presentan serias deficiencias que pueden acarrear en la pérdida de datos, tiempo, dinero e información, entre otros, por lo tanto, se justifica que la Municipalidad debe contar y aplicar un plan de seguridad informática.
2. Se realizó un análisis de la situación actual y se identificó las funciones del personal que labora en conjunto con la infraestructura tecnológica, por lo que se efectuó el desarrollo de este plan de seguridad informático, a esto se llegó que ahora municipalidad ya tiene en documentos este diseño de un plan de seguridad informática, el cual es muy importante tener hoy en día las municipalidades o empresas públicas y privadas.
3. Se diseñó una propuesta tecnológica para tener una mayor seguridad informática en la municipalidad distrital de Canchaque, según mi persona este diseño está pensado únicamente para dicha municipalidad por los procesos y actividades que se desarrollaron a lo largo del 2020, por lo tanto, tuve el privilegio de concluir con mi trabajo de investigación exitosamente por lo tanto, se concluye que la planificación y ejecución de la elaboración de un plan de seguridad informática permitirá salvaguardar los activos de la municipalidad.

RECOMENDACIONES

1. Se le hace recomendación respectiva al equipo técnico de la municipalidad de Canchaque hacer una inspección cada cierto tiempo sus computadoras y ejecutar la revisión de los riesgos y amenazas ya que hoy en día la tecnología se actualiza a cada momento y debe ser vigilada para eludir inconvenientes a futuro.
2. Se sugiere al área de la gerencia, de la municipalidad establecer perfiles para los contratos adecuados de los profesionales los cuales tendrán la función de revisión e implementación de este plan de seguridad informático para la municipalidad la cual pueda ser de gran utilidad si se llegara a ser implementada.
3. Para mayor eficiencia en las soluciones de las vulnerabilidades encontradas le recomendamos al alcalde de la municipalidad distrital de Canchaque, crear un departamento de informática lo cual se logrará que los equipos tecnológicos reciban actualizaciones de calidad y seguridad para no tener dificultades técnicas con respecto a las computadoras.
4. Asimismo, le hago presente al área de capacitaciones y charlas, esta recomendación fundamental la cual consiste en brindar capacitaciones al personal que labora en la municipalidad sobre el cumplimiento de las normas de seguridad ISO 27001.
5. Se recomienda al alcalde de la municipalidad distrital de Canchaque actualizar, renombrar y restablecer los puntos de señalizaciones de seguridad en los ambientes tecnológicos y sus laboratorios donde se utilizan computadoras, impresoras, entre otros y también oficinas de secretaria.
6. Como ultima recomendación hacia el alcalde de la municipalidad distrital de Canchaque, de seguir los protocolos establecidos en el uso en los equipos tecnológicos para sacar su 100% de los equipos tecnológicos y a esto sumarle los protocolos sanitarios sobre la salud por el contagio de covid-19, en espacios sin ventilación.

REFERENCIAS BIBLIOGRÁFICAS

1. Correa A. J., Mendoza R.A., Meléndez J.I., Análisis y diseño de un sistema para la gestión de archivos de la oficina de normalización previsional. Lima, Perú - setiembre, 2017.
2. Ríos L. M., Evaluación al control informático en el proceso de ventas y su incidencia en la rentabilidad de la empresa Megamultisuelas en el segundo semestre del año 2017, Ambato – ecuador, 2017.
3. Chávez V. H., sistema de información para el control, seguimiento y mantenimiento del equipamiento hospitalario, lima – Perú, 2016.
4. Sánchez V. E. y Vargas R. M., análisis y diseño de edificios de concreto armado considerando la rigidez efectiva de sus elementos estructurales, lima, 27 de noviembre de 2018.
5. Soto R. J., implementación de un sistema de información basado en web 2.0 para la mejora de la calidad de servicio en la empresa Etno producciones, Huancayo – Perú, 2018.
6. Oré E. D. y Valverde O. A., análisis y diseño de un sistema de control de producción para compañías manufactureras textiles lima, Perú 2017.
7. Mendoza M. A. Sistema web de registro y búsqueda de incidencias en el área de soporte técnico para la municipalidad provincial de Piura, Piura – Perú 2019.
8. Saavedra A., análisis y diseño de un sistema e-commerce para la gestión de ventas: caso empresa world of cakes Piura, noviembre de 2016.
9. Caminati M. A. y caqui R. C. Análisis y diseño de sistemas de tratamiento de agua para consumo humano y su distribución en la universidad de Piura, Piura, abril de 2013.
10. Romero M. I., Figueroa Moràn g. L., vera d. S., Álava Cruzatty j. E., parrales G. R., Álava C. J., Murillo A. L. y Castillo M. A., Introducción a la Seguridad informática y el análisis de vulnerabilidades área de innovación y desarrollo, s.l., primera edición: alcoy (alicante) octubre 2018.
11. Andrada A. Nuevas tecnologías de la información y la comunicación ntiex argentina: editorial maipue; 2004.

12. Catherine M. R., Bases de datos primera edición. México – monterrey. 2015.
13. Hernández A., Los sistemas de información: evolución y desarrollo, departamento de economía y dirección de empresas universidad de zaragoza, 2012.
14. Tanenbaum A.S.: modern operating systems (3rd edition), prentice-hall, 2008. Edición en castellano: sistemas operativos modernos (3ra edición). Pearson educación, 2009.
15. Molina F.J. Redes locales Madrid-España: rama; 2014.
16. Rumbaugh J., Jacobson i. y Booch g. El lenguaje unificado de modelado. Manual de referencia, Pearson educacion. S.a. Madrid – 2000.
17. Fernández T., Pita C.; Días P. Investigación cuantitativa y cualitativa. España; 2002.
18. Sáez LJM. Investigación educativa: fundamentos teóricos, procesos y elementos prácticos: enfoque práctico con ejemplos, esencial para TFG, TFM y tesis Madrid-España: UNED - Universidad Nacional de Educación a Distancia; 2017.
19. Hernández R.; Fernández C. Baptista M.P. Metodología De La Investigación. V. Chacón JM, editor. México: McGraw-Hill; 2010.
20. Pazmiño C. I. Tiempo de investigar, investigación científica 2: cómo hacer una tesis de grado Quito, Ecuador: EDITEKA Ediciones; 2008.
21. Kevin D. M. y William L. S., El arte de la Intrusión, edición original publicada por RA-MA Editorial, Madrid, España
22. Osorio M., II Congreso Internacional de Transformación Educativa, alternativas para nuevas prácticas educativas, libro 3. Las tecnologías de la información y la comunicación (TIC): Avances, retos y desafíos en la transformación educative, 2015.
23. Fowler M. y Kendall S., UML gota a gota, addison wesley longman de México, S.A. de C.V., Naucalpan de Juárez México 1999.
24. Bastidas J. Presentada por: javier bastidas parraga. 2016;108.
25. MAGERIT– versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Minist Hacienda y Adm Públicas [Internet]. 2012;2006(630-12-171-8):127. Disponible en:

<https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html>

26. Alfaro I., Vargas E.. Diseño del plan de seguridad informática del sistema de información misional de la procuraduría general de la nación. 2016;(june).
27. Evelyn A., Santiago G. Tecnologías de la información y la comunicación. Cual Informática [Internet]. 2015;76. Disponible en: <http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/1189/Libro TIC %282%29-1-76 %281%29.pdf?sequence=1&isAllowed=y>
28. Martínez F. J. Análisis y diseño de un sistema de control de asistencia para la panificadora “Pan de Dios”–Tumbes; 2017. (Tesis para optar el título profesional de Ingeniero de Sistemas). Universidad Católica Los Ángeles de Chimbote. Piura; 2017.
29. Siancas B. J. C. "Análisis, diseño e implementación de un sistema de gestión del equipamiento hospitalario para el hospital universitario". Universidad nacional de Piura, Piura – Perú, 2016.
30. Ortiz L. J. C., Ramos M. y Sullon G. J., Análisis, diseño y elaboración de un prototipo para un sistema de administración y elección de rutas de transporte público, Escuela Profesional de Ingeniería Informática, Universidad nacional de Piura, Piura – Perú, 2020.
31. Muñoz J. “Diseño de políticas de seguridad informática para la dirección de tecnologías de la información y comunicación (DTIC) de la universidad de cuenca”. facultad de ingeniería, Cuenca – Ecuador, 2016.
32. Hernández R. y otros. “Metodología de la investigación. McGraw Hill, Editorial Iberoamérica. México, 2003.
33. Gil J.A. Técnicas e instrumentos para la recogida de información [En Línea]. Madrid: UNED - Universidad Nacional de Educación a Distancia, 2016 [consultado 15 May 2021]. Disponible en: <https://elibro.net/es/ereader/uladech/48876?page=20>
34. Romero A., SEGURIDAD INFORMÁTICA Y ALTA DISPONIBILIDAD, ESPAÑAIES TIEMPOS MODERNOS; Zaragoza – ESPAÑA.
35. Zapata P. D. M., Formación de Seguridad informática, una visión global, CEO of Iberlayer, Universidad politécnica de Madrid, 2018.

36. Noruega A., Implementación de un sistema de detección de intrusos para venezolana del vidrio C.A., Caracas, octubre de 2019:79-1.
37. Arenal L. C. Gestión de la prevención de riesgos laborales en pequeños negocios. MF1792 [En Línea]. Logroño, La Rioja: Editorial Tutor Formación, 2017 [consultado 15 Oct 2021]. Disponible en: <https://elibro.net/es/ereader/uladech/44233?page=76>
38. Talavera L., ¿Qué es el Activo de una empresa?, Madrid, España: Billin [Internet]. 2021. Disponible en: <https://www.billin.net/glosario/definicion-activo/#:~:text=Se%20define%20el%20Activo%20de,esperamos%20tener%20un%20beneficio%20futuro.>
39. Uladech, Código de ética para la investigación, Versión 003, Chimbote – Perú; 2020. Disponible en: <https://www.uladech.edu.pe/images/stories/universidad/documentos/2019/reglamento-comite-etica-v003.pdf>
40. ISO 27001:2013, Guía de Implantación para la seguridad de la Información; 4 octubre 2020. [En línea]. Available: <https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf>
41. ISO Tools, ISO 27001:2013: Motivos para conocer mejor la nueva norma, Blog especializado en Sistemas de Gestión, 4 octubre 2020. [En línea]. Disponible en: <https://www.pmg-ssi.com/norma-27001/>

Anexos

Anexo 1: Cronograma de actividades

CRONOGRAMA DE ACTIVIDADES																
N°	Actividades	Año 2021								Año 2022						
		Semestre I				Semestre II				Semestre I				Semestre II		
		Marzo-Junio				Septiembre - Diciembre				Marzo-Junio				Septiembre - Diciembre		
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3
1	Elaboración del Proyecto	x														
2	Revisión del proyecto por el Jurado de Investigación		x													
3	Aprobación del proyecto por el Jurado de Investigación			x												
4	Exposición del proyecto al Jurado de Investigación o Docente Tutor				x											
5	Mejora del marco teórico		x	x												
6	Redacción de la revisión de la literatura.			x												

Anexo 2: Presupuesto.

Presupuesto desembolsable (Estudiante)			
Categoría	Base	Costo Unitari	Total
Suministros			
• Impresiones	0.50	34	17.00
• Fotocopias	0.10	20	6.00
• Anillado	15.00	1	15.00
• Papel A-4	0.10	100	15.00
• Lapiceros	2.00	4	08.00
Servicios			
• Uso de Turnitin	50.00	1	50.00
Gastos de viaje			
• Pasajes interprovinciales	15.00	2	30.00
• Pasajes locales	2.00	4	08.00
Total, de presupuesto desembolsable			149
Presupuesto no desembolsable (Universidad)			
Categoría	Base	Costo unitario	Total
Servicios			
Uso de Internet Laboratorio de Aprendizaje Digital - LAD)	50.00	1	50.00
Búsqueda de información en base de datos	00.00	0	00.00
Recurso humano			
Asesoría personalizada	00.00	0	00.00
Total, de presupuesto no desembolsable			50.00
Total (S/.)			199.00

Anexo 3: Cuestionario.

CUESTIONARIO

TITULO:

ANÁLISIS Y DISEÑO DE UN PLAN DE SEGURIDAD INFORMÁTICA EN LA MUNICIPALIDAD DISTRITAL DE CANCHAQUE – PIURA; 2020.

INSTRUCCIONES:

Solicitamos su colaboración, respondiendo con sinceridad el presente cuestionario.

El cuestionario tiene por objetivo conocer sobre los sistemas de gestión basados en la norma ISO/IEC 27001 para la seguridad de información. En este instrumento se presentarán 10 preguntas, que deben ser desarrolladas marcando SI o NO según considere la alternativa correcta.

EJEMPLO:

PREGUNTAS	SI	NO
¿RESPONDERA LAS PREGUNTAS CON SINCERIDAD?	<input checked="" type="checkbox"/>	<input type="checkbox"/>

CUESTIONARIO:

Nivel de satisfacción respecto a la seguridad informática actual	SI	NO
¿Existe en dicha Municipalidad un responsable del área de la seguridad informática?	<input type="checkbox"/>	<input type="checkbox"/>
¿Ha ocurrido algún incidente de seguridad informática en su puesto de trabajo en el último año?	<input type="checkbox"/>	<input type="checkbox"/>
¿Cree que el sistema de gestión basado en la ISO 27001 ayudara en la seguridad de información en la Municipalidad de Canchaque?	<input type="checkbox"/>	<input type="checkbox"/>
¿Cree Usted que una charla como esta sea de mucha importancia?	<input type="checkbox"/>	<input type="checkbox"/>
¿Cree que es necesario aplicar controles de seguridad para evitar robo o daño de información importante para la Municipalidad Distrital de Canchaque?	<input type="checkbox"/>	<input type="checkbox"/>
Nivel de aceptación de la propuesta de mejora	SI	NO
¿Conoce Usted sobre el tema de seguridad informática?	<input type="checkbox"/>	<input type="checkbox"/>
¿Considera que la seguridad de información debe ser vital en la Municipalidad?	<input type="checkbox"/>	<input type="checkbox"/>
¿Considera que la Municipalidad le da importancia suficiente a la seguridad informática?	<input type="checkbox"/>	<input type="checkbox"/>
¿Conoce Usted sobre la norma ISO 27001 en la seguridad de información?	<input type="checkbox"/>	<input type="checkbox"/>
¿La Municipalidad imparte constantemente capacitaciones de seguridad informática y la norma ISO 27001?	<input type="checkbox"/>	<input type="checkbox"/>

Anexo 4: Consentimiento informado



PROTOCOLO DE CONSENTIMIENTO INFORMADO PARA ENCUESTAS (Ingeniería y Tecnología)

La finalidad de este protocolo en Ingeniería y tecnología es informarle sobre el proyecto de investigación y solicitarle su consentimiento. De aceptar, el investigador y usted se quedarán con una copia.

La presente investigación se titula ANÁLISIS Y DISEÑO DE UN PLAN DE SEGURIDAD INFORMÁTICA EN LA MUNICIPALIDAD DISTRITAL DE CANCHAQUE – PIURA; 2020. y es dirigido por Cutin Zapata Alipio, investigador de la Universidad Católica Los Ángeles de Chimbote.

El propósito de la investigación es: Medir el Nivel de satisfacción de trabajadores que conforman el distrito y también Nivel de satisfacción del análisis y diseño de seguridad informática De la Municipalidad. Para ello, se le invita a participar en una encuesta que le tomará 3 minutos de su tiempo. Su participación en la investigación es completamente voluntaria y anónima. Usted puede decidir interrumpirla en cualquier momento, sin que ello le genere ningún perjuicio. Si tuviera alguna inquietud y/o duda sobre la investigación, puede formularla cuando crea conveniente.

Al concluir la investigación, usted será informado de los resultados a través del correo alipioresuelto@gmail.com para recibir mayor información. Asimismo, para consultas sobre aspectos éticos, puede comunicarse con el Comité de Ética de la Investigación de la universidad Católica los Ángeles de Chimbote.

Si está de acuerdo con los puntos anteriores, complete sus datos a continuación:

Nombre: _____

Fecha: _____

Correo electrónico: _____

Firma del participante: _____

Firma del investigador (o encargado de recoger información):  _____

COMITÉ INSTITUCIONAL DE ÉTICA EN INVESTIGACIÓN – ULADECH CATÓLICA

Anexo 5: Carta de aceptación.



"Año de la universalización de la salud"

SOLICITO: APLICAR ENCUESTAS
POR TEMA DE ESTUDIO
UNIVERSITARIO

SEÑOR ALCALDE DE LA MUNICIPALIDAD DE CANCHAQUE

Yo, **CUTIN ZAPATA ALIPIO** identificado con DNI 71533432, Alumno de la Universidad Católica Los Ángeles de Chimbote con código N° 0809181121, con el debido respeto me presento y expongo:

Que, siendo un requisito indispensable para culminar el 6to ciclo de la carrera Ing. De sistemas, aplicar 10 encuestas anónimas por trabajadores de esta municipalidad, para un trabajo de temas de estudio, los cual serán respuestas anónimas y solo se utilizaran para tabular; de tal manera puedo recalcar que es solo para tema de estudio.

POR LO EXPUESTO.

Solicito a usted acceda a mi petición por ser tema de estudio.

Canchaque, 19 de octubre de 2020.

Atentamente.

CUTIN ZAPATA ALIPIO

DNI N° 71533432
CELULAR N° # 928280755

Anexo 6: Validez de expertos.

FICHA DE VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1 Nombres y apellidos del validador : Ivan Martin Perez Faefan
 1.2 Cargo e institución donde labora : Docente Tutor - Cesar Vallejo
 1.3 Nombre del instrumento evaluado : Enquesta
 1.4 Autor del instrumento : Cutia Zapata Alpio

II. ASPECTOS DE VALIDACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (X), según la calificación que asigna a cada uno de los indicadores.

1. Deficiente (Si menos del 30% de los ítems cumplen con el indicador).
 2. Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador).
 3. Buena (Si más del 70% de los ítems cumplen con el indicador).

Criterios	Aspectos de validación del instrumento Indicadores	1	2	3	Observaciones Sugerencias
		D	R	B	
• PERTINENCIA	Los ítems miden lo previsto en los objetivos de investigación.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• COHERENCIA	Los ítems responden a lo que se debe medir en la variable y sus dimensiones.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• CONGRUENCIA	Los ítems son congruentes entre sí y con el concepto que mide.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• SUFICIENCIA	Los ítems son suficientes en cantidad para medir la variable.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• OBJETIVIDAD	Los ítems se expresan en comportamientos y acciones observables.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• CONSISTENCIA	Los ítems se han formulado en concordancia a los fundamentos teóricos de la variable.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• ORGANIZACIÓN	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• CLARIDAD	Los ítems están redactados en un lenguaje entendible para los sujetos a evaluar.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• FORMATO	Los ítems están escritos respetando aspectos técnicos (tamaño de letra, espaciado, interlineado, nitidez).	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• ESTRUCTURA	El instrumento cuenta con instrucciones, consignas, opciones de respuesta bien definidas.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
CONTEO TOTAL (Realizar el conteo de acuerdo a puntuaciones asignadas a cada indicador)					
		C	B	A	Total

Coefficiente de validez : $\frac{A+B+C}{30} = \frac{30+0+0}{30} = 1$

III. CALIFICACIÓN GLOBAL

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado.

Intervalos	Resultado
0,00 - 0,49	• Validez nula
0,50 - 0,59	• Validez muy baja
0,60 - 0,69	• Validez baja
0,70 - 0,79	• Validez aceptable
0,80 - 0,89	• Validez buena
0,90 - 1,00	• Validez muy buena

Validez muy buena

16/10/2020

REG. CIP: Nº 221790

FICHA DE VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

- 1.1 Nombres y apellidos del validador : BRISIA ENZARTE LYRIVERA MORALES
 1.2 Cargo e institución donde labora : DOCENTE UNIVERSITARIO - ULADECH
 1.3 Nombre del instrumento evaluado : ENCUESTA
 1.4 Autor del instrumento : CUTIN ZAPATA ALIPIO

II. ASPECTOS DE VALIDACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (X), según la calificación que asigna a cada uno de los indicadores.

1. Deficiente (Si menos del 30% de los ítems cumplen con el indicador).
 2. Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador).
 3. Buena (Si más del 70% de los ítems cumplen con el indicador).

Criterios	Aspectos de validación del instrumento Indicadores	1 2 3			Observaciones Sugerencias
		D	R	B	
• PERTINENCIA	Los ítems miden lo previsto en los objetivos de investigación.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• COHERENCIA	Los ítems responden a lo que se debe medir en la variable y sus dimensiones.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• CONGRUENCIA	Los ítems son congruentes entre sí y con el concepto que mide.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• SUFICIENCIA	Los ítems son suficientes en cantidad para medir la variable.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• OBJETIVIDAD	Los ítems se expresan en comportamientos y acciones observables.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• CONSISTENCIA	Los ítems se han formulado en concordancia a los fundamentos teóricos de la variable.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• ORGANIZACIÓN	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• CLARIDAD	Los ítems están redactados en un lenguaje entendible para los sujetos a evaluar.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• FORMATO	Los ítems están escritos respetando aspectos técnicos (tamaño de letra, espaciado, interlineado, nitidez).	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• ESTRUCTURA	El instrumento cuenta con instrucciones, consignas, opciones de respuesta bien definidas.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
CONTEO TOTAL					
(Realizar el conteo de acuerdo a puntuaciones asignadas a cada indicador)		C	B	A	Total

Coefficiente de validez : $\frac{A + B + C}{30} = \frac{30 + 0 + 0}{30} = 1$

III. CALIFICACIÓN GLOBAL

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado.

VALIDEZ MUY BUENA

15/10/2020

Intervalos	Resultado
0,00 – 0,40	• Validez nula
0,50 – 0,59	• Validez muy baja
0,60 – 0,69	• Validez baja
0,70 – 0,79	• Validez aceptable
0,80 – 0,89	• Validez buena
0,90 – 1,00	• Validez muy buena


 Brisia EnzarTE Lyrivera Morales
 DOCENTE UNIVERSITARIO
 ULADECH

FICHA DE VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1 Nombres y apellidos del validador : Pucy Robin Bravo Baldon
 1.2 Cargo e institución donde labora : Docente - Cusan Valijo
 1.3 Nombre del instrumento evaluado : Instrumento de Resolución de Datos
 1.4 Autor del instrumento : Culín Zapate Alipio

II. ASPECTOS DE VALIDACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (X), según la calificación que asigna a cada uno de los indicadores.

1. Deficiente (Si menos del 30% de los ítems cumplen con el indicador).
2. Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador).
3. Buena (Si más del 70% de los ítems cumplen con el indicador).

Criterios	Aspectos de validación del instrumento Indicadores	1	2	3	Observaciones Sugerencias
		D	R	B	
• PERTINENCIA	Los ítems miden lo previsto en los objetivos de investigación.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• COHERENCIA	Los ítems responden a lo que se debe medir en la variable y sus dimensiones.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• CONGRUENCIA	Los ítems son congruentes entre sí y con el concepto que mide.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• SUFICIENCIA	Los ítems son suficientes en cantidad para medir la variable.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• OBJETIVIDAD	Los ítems se expresan en comportamientos y acciones observables.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• CONSISTENCIA	Los ítems se han formulado en concordancia a los fundamentos teóricos de la variable.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• ORGANIZACIÓN	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• CLARIDAD	Los ítems están redactados en un lenguaje entendible para los sujetos a evaluar.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• FORMATO	Los ítems están escritos respetando aspectos técnicos (tamaño de letra, espaciado, interlineado, nitidez).	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
• ESTRUCTURA	El instrumento cuenta con instrucciones, consignas, opciones de respuesta bien definidas.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
CONTEO TOTAL					
(Realizar el conteo de acuerdo a puntuaciones asignadas a cada indicador)		C	B	A	Total

Coefficiente de validez : $\frac{A+B+C}{30} = \frac{30+0+0}{30} = 1$

III. CALIFICACIÓN GLOBAL

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado.

Validez muy buena

14/10/2020

Intervalos	Resultado
0.00 - 0.49	• Validez nula
0.50 - 0.59	• Validez muy baja
0.60 - 0.69	• Validez baja
0.70 - 0.79	• Validez aceptable
0.80 - 0.89	• Validez buena
0.90 - 1.00	• Validez muy buena



Res. CIP N° 9269 L

Anexo 6: Prueba piloto.

Preguntas											
Individuos	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	
1	0	1	1	1	1	1	1	1	1	0	8
2	1	0	0	1	1	0	0	0	1	0	4
3	0	0	1	1	1	1	1	1	1	0	7
4	0	1	0	1	1	1	0	0	1	0	5
5	0	0	1	1	1	1	1	1	1	0	7
6	0	0	0	0	1	0	0	0	1	0	2
7	0	1	1	0	1	1	1	1	1	0	7
8	0	1	0	0	1	0	0	0	1	0	3
9	0	0	1	1	1	1	1	1	1	0	7
10	0	0	0	0	1	0	0	0	1	0	2
Totales	1	4	5	6	10	6	5	5	10	0	
p	0.1	0.4	0.5	0.6	1	0.6	0.5	0.5	1	0	
q	0.9	0.6	0.5	0.4	0	0.4	0.5	0.5	0	1	
p*q	0.1	0.24	0.25	0.24	0	0.2	0.25	0.25	0	0	
$\sum(p*q)$	1.6										
σ^2	5.3										
K	10										

Donde:	
K=	Numero de Items del instrumento
p=	Porcentaje de personas que responde correctamente cada item
q=	Porcentaje de personas que responde incorrectamente cada item
σ^2 =	Varianza total del instrumento

KR-20	Interpretación
1	si
0	no

$(k/K-1) =$	1.11
$1-(\sum pq/\sigma^2) =$	0.71
KR-20	0.78