UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE

FACULTAD DE CIENCIAS E INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE UN PLAN DE SEGURIDAD INFORMÁTICO EN EL JUZGADO DE PAZ DE ÚNICA NOMINACIÓN DEL DISTRITO DE CANCHAQUE – PIURA, 2021.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR

CUTIN ZAPATA, ALIPIO

ORCID: 0000-0002-1714-3089

ASESORA

SUXE RAMIREZ, MARIA ALICIA

ORCID:0000-0002-1358-4290

PIURA – PERÚ

2022

EQUIPO DE TRABAJO

AUTOR

Cutin Zapata, Alipio

ORCID: 0000-0002-1714-3089

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

ASESOR

Suxe Ramírez, María Alicia

ORCID: 0000-0002-1358-4290

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

JURADO

Ocaña Velásquez Jesús Daniel

ORCID: 0000-0002-1671- 429X

Torres Ceclén Carmen Cecilia

ORCID: 0000-0002-8616-7965

Ancajima Miñan Víctor Ángel

ORCID: 0000-0002-3122-4512

JURADO EVALUADOR DE TESIS Y ASESOR

DR. JESÚS DANIEL OCAÑA VELÁSQUEZ
PRESIDENTE

DRA. CARMEN CECILIA TORRES CECLÉN
MIEMBRO

DR. VÍCTOR ÁNGEL ANCAJIMA MIÑAN
MIEMBRO

DRA. MARÍA ALICIA SUXE RAMÍREZ
ASESORA

DEDICATORIA

A mis padres Pablo y Rosa quienes esfuerzo me han permitido llegar a culminar hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo, valentía y respeto, de no tener miedo las adversidades porque Dios está conmigo siempre.

A mi hermano Alberto por apoyo incondicional, durante todo este proceso, de mis estudios, por estar conmigo en todo momento gracias.

Alipio Cutin Zapata

AGRADECIMIENTO

Quiero expresar mi gratitud al Juez de Paz por abrirme sus puertas en el proceso de esta investigación y a Dios, quien con su bendición todos se encamina por el bien.

De igual manera mis agradecimientos a la Universidad Católica Los Ángeles De Chimbote, a toda la Facultad de Ingeniería de sistemas, a mi docente Ancajima Miñán Víctor quien con la enseñanza de sus valiosos conocimientos hicieron que pueda crecer día a día como profesional, gracias a cada una de ustedes por su paciencia, dedicación, apoyo incondicional y amistad.

Alipio Cutin Zapata

RESUMEN

Esta tesis fue elaborada mediante la línea de investigación: Sistemas de gestión de la calidad y seguridad de la información; utilizando la metodología MAGERIT, además se identificó que el problema del Juzgado de paz de única nominación Canchaque los documentos se pueden extraviar, borran o se pierden, para ello se propuso el objetivo principal de implementar un plan de seguridad informática en el Juzgado de Paz de única nominación Canchaque con la finalidad de mantener segura la información del Jugado, como alcance de la presente investigación da beneficio al Juez, las personas que adquieren los servicios del Juzgado, esta investigación tuvo un enfoque cuantitativo de tipo descriptivo, de diseño no experimental de corte transversal; la población consta de 7757 personas, pero se tomó la muestra por conveniencia de 20 personas de las cuales 3 son trabajadores y 17 adquieren los servicios con frecuencia, se utilizó el instrumento de encuesta como método de recolección de datos, por lo que se obtuvo en la primera dimensión indica que el 100.00% si está satisfecho con la propuesta de implementación del pan de seguridad información, en la segunda dimensión se aprecia que el 65.00% no conoce sobre las TIC, la presente investigación concluye que la implementación de un plan de seguridad informática en el Juzgado de Paz en Canchaque, permitirá salvaguardar la integridad de la información.

Palabras clave: MAGERIT, Plan de seguridad, Seguridad de información.

ABSTRACT

This thesis was prepared through the line of research: Quality management systems and information security; using the MAGERIT methodology, it was also identified that the problem of the single-nomination Justice of the Peace Canchaque documents can be lost, deleted or lost, for this the main objective is to implement an information security plan in the Justice of the Peace of The only Canchaque nomination in order to keep the information of the Court safe, as the scope of this investigation benefits the Judge, the people who acquire the services of the Court, this research had a quantitative approach of a descriptive type, with a non-experimental cross-sectional design; the population consists of 7757 people, but the sample was taken for convenience of 20 people, of which 3 are workers and 17 frequently acquired the services, the survey instrument was obtained as a data collection method, for which it was obtained in the first dimension indicates that 100.00% are satisfied with the proposed implementation of the information security plan, in the second dimension it can be seen that 65.00% do not know about TIC, this research concludes that the implementation of a security plan information technology in the Justice of the Peace in Canchaque, will allow to save the integrity of the information.

Keywords: MAGERIT, Security plan, Information Security.

ÍNDICE DE CONTENIDO

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

I. INTRODUCCIÓN

La seguridad informática, en general, está teniendo una importancia cada vez mayor. Los usuarios, particulares y trabajadores de las empresas, deben ser conscientes de que el funcionamiento correcto de sus sistemas depende en gran medida, de protegerlos como el mayor de sus tesoros (1).

En el juzgado de paz de única nominación de Canchaque es una institución del estado que tiene como función velar por los intereses del pueblo ayudando al bienestar de la población, actualmente en el despacho del juzgado se realizan diversas actividades como documentación y legalización de documentos diferentes como diversos tipos de actos jurídico donaciones, compra y venta, alquiler, autorizaciones de viajes a menores de edad entre otros documentos, al momento de realizar estas diversas actividades se usan impresiones, copias, tipeos, borrar, extraer, redactar y modificar documentos de mucha importancia, en el despacho aún no se actualizan los riesgos y amenazas como lo requiere la ISO 27001 y los procesos de atender a la población de dicho distrito es de un tiempo determinado el cual se prolonga porque la PC y el internet no son lo suficientemente rápido.

¿La implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura mejora el control de datos e información?

Como objetivo general Implementar un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura; 2021, para mejorar el control de datos e información y como objetivos específicos: Determinar el nivel de conocimiento acerca de la seguridad informática del juzgado de paz de única nominación, analizar la seguridad informática del juzgado de paz de única nominación e implementar un plan de mejora de seguridad informática en el juzgado de paz de única nominación.

Se justifica operativamente ya que con este sistema informático el juzgado de paz de única nominación de Canchaque dará lugar a que sus procesos sean más rápidos

y realizará sus atenciones a la población con mayor eficiencia y fluidez, se justifica tecnológicamente porque esta implementación en el plan de seguridad informático el despacho contara con un servicio de calidad, para acelerar los procesos ya que en el mundo que estamos viviendo el uso de las Tics es cada vez mayor, poniendo en contexto que ahora todas las empresas o instituciones deben estar actualizadas y capacitadas sobre las nuevas tecnologías y se justifica económicamente ya que este plan de seguridad informática en el juzgado de paz de única nominación Canchaque brindará menor consumo de energía, tinta, lapiceros, hojas y mantenimiento por lo cual será de menor costo, ahorrando tiempo y dinero. El tipo de metodología desarrollada es de tipo cuantitativo nivel descriptiva y de diseño no experimental de corte trasversal.

En la dimensión Nro. 1 “Nivel de satisfacción de la implementación de un plan de seguridad informático”, se obtuvo la aprobación por parte de los encuestados con un grado de certeza del 100% y la dimensión Nro. 2 “Nivel de conocimiento con respecto al uso de las herramientas TIC” se obtuvo que carecen de un poco de conocimiento sobre las tecnologías de la información, ya que los resultados obtenidos de los encuestados fueron de 65.00% No conocían sobre las herramientas Tic y el 35.00% si conocía.

Se concluye que la evaluación actual del juzgado de paz de única nominación es deficiente por los riesgos y amenazas que tienen sus activos, por ello se identificaron y registraron, además se determinó el nivel de conocimiento acerca de la seguridad informática actual del juzgado de paz de única nominación y se implemente el plan de seguridad informática en el juzgado de paz de única nominación Canchaque.

II. REVISÓN DE LA LITERATURA

2.1 Antecedentes

2.1.1 Antecedentes a nivel internacional

Según Torres (2), en el año 2020 en su tesis titulada “Plan de seguridad informática basado en la norma ISO 27001, para proteger la información y activos de la empresa privada MEGAPROFER S.A.”; se utilizó una muestra de 4 personas y se realizó una entrevista y encuesta realizada al personal TIC, elaborada en base a los estándares de seguridad TI basados en la norma ISO 27001:2013, los resultados que arrojo fue que el 10% de su conocimiento es bueno, el 0% es regular, el
15% de su conocimiento es muy pobre y el 35% cuneta sin conocimiento. El departamento no cuenta con altos conocimientos en seguridad de la información, según evaluación de conocimientos en seguridad de la información, procedimientos de defensa y seguridad de la información, y aplicación de herramientas de protección de datos y seguridad de la información, así como un servidor de Backups.

Según Chicaiza y Vinicio (3), en el año 2020 en su tesis titulada “Plan De Seguridad Informática Basado En La Norma ISO 27001, Para Proteger La Información Y Activos De La Empresa Privada Megaprofer S.A.”; se utilizó la metodología MAGERIT con una muestra de 4 personas a los cuales se les aplico una entrevista y encuesta al personal, el cual obtuvo que el 77,80% y también que el 75% en mantener la gestión adecuada para que los activos no sean manipulados, La entidad no cuenta con procedimientos efectivos para proteger la información, los diversos procesos que implementan ciertas políticas ineficaces que no permiten un cumplimiento aceptable pueden garantizar la confidencialidad, integridad y disponibilidad de la información. Es fundamental contar con una matriz de riesgos, que ayude a definir la información disponible. vulnerabilidades en los activos de información. Con el modelo SGSI integrado en la norma ISO

27001, existe un proceso continuo de gestión de la seguridad que puede reducir o eliminar el riesgo de la información.

Según Huincho y Nuñez (20), en el año 2019 en su tesis titulada "Sistema De Gestión De Seguridad De La Información Para Mejorar La Protección Informática De La Comisaria Región Huancavelica" hicieron uso de la metodología MAGERIT, se utilizó como instrumento de recolección de datos la encuesta, observación y entrevista, como principales resultados tiene que al 87% Reducirá y mitigará los riesgos de los activos de la información además se ha logrado al 93% para gestionar, monitorear, de manera eficiente los incidentes y vulnerabilidades de seguridad de la información Los usuarios potenciales de la comisaria PNP de la región de Huancavelica y de una manera general de nuestra institución, deberán ser capaces de superar el problema cultural, de sobreponerse al temor natural y apreciar el horizonte de utilidades, aplicaciones, así como del ahorro de tiempo y dinero, que nos ofrecen la seguridad de la información, lo cual será posible a partir de una adecuada implementación y capacitación.

2.1.2 Antecedentes a nivel nacional

Según Machicao (4), en el año 2019 en su tesis titulada "Análisis de riesgo y políticas de seguridad de información de la oficina de tecnologías de información (OTI) – UNA PUNO 2018"; 12 personas divididas en cada sub área, incluyendo a la jefa de la OTI, se aplicó el método de análisis de riesgo, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, el 76.19% respecto al activo hardware, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo bajo y 95.24 % respecto al activo de acceso a internet, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo bajo, de acuerdo al resultado de análisis de riesgo de la seguridad de la información respecto a los activos primordiales de la Oficina de

Tecnologías de Información, existen 12 riesgo de nivel alto, 28 riesgos de nivel medio y 151 riesgos de nivel bajo, siendo varios los criterios respecto a las amenazas que puedan vulnerar la información que administra la OTI, que permite delimitar el su estructura, siendo hoy en día la información en todas sus formas un activo primordial, al cual debe garantizarse su confidencialidad, integridad y disponibilidad.

Según Aguirre (5), en el año 2018 en su tesis titulada "Sistema web para la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en la empresa de servicios informáticos S.A.C – La Molina" la población está conformada por la cantidad de informes diarios de backup de clientes, siendo estos una cantidad de 30 informes en un periodo de 30 días, se utilizó el instrumento de recolección de datos utilizado fue con las Fichas de Registro, los datos obtenidos de antes de la implementación del sistema Web, se encontró una media de 77.39 % mientras que para los datos obtenidos después de la implementación del sistema web se encontró una media de 96.67 %, concluyo que se ha comprobado que el Porcentaje de Reportes entregados en el plazo establecido, utilizando el sistema web en la gestión de la seguridad de la información de la empresa Servicios Informáticos S.A.C. aumentó, sin el sistema web la media fue de 72.33% y con uso del sistema web la media fue de 97.94, logrando un aumento de 25.61%.

Según Celis (6), en el año 2018 en su tesis titulada "plan de seguridad de la información aplicado a la central hidroeléctrica Carhuaquero"; se usó una muestra de 36 usuarios donde se aplicó encuestas y se utilizó la metodología MAGERIT, Cada proceso de trabajo conlleva a riesgos de Incendio o explosiones perfectamente identificados, por ello es necesario conocerlo y protegerlo, por ello la presencia de la brigada, la cual debe tener un 100% de conocimientos que nos ayudarán a la prevención y la amenaza de mayor relevancia es el Fuego con un 60% en afectación de la disponibilidad, De todos los activos que conforman

UPH. Carhuaquero, se han establecido 25 activos de carácter “crítico” que representan el 40,98% de todos los activos encontrados. Por otro lado, entre las amenazas encontradas, se han establecido 15 de carácter “Muy Alto” que equivalen al 30% del total de ellas.

2.1.3 Antecedentes a nivel regional

Según Solano (7), en el año 2018 en su tesis titulada “Implementación de un sistema informático de hospitalización del hospital Elpidio Berovides Pérez – Otuzco; 2018.”; se utilizó una muestra de 25 personas entre ellas médicos, enfermeras y administrativos a los cuales se le aplico encuestas, el 100.00% del personal, NO cuentan un sistema eficiente para el área de hospitalización y el 84.00% del personal, SI manifiesta que es necesario de mejorar los procesos en el área de hospitalización, mientras que 16.00%, indica que NO, Según los resultados obtenidos, analizados y debidamente interpretados, se concluye que existe la necesidad de implementar un sistema informático de hospitalización debido a insatisfacción de los trabajadores, por el sistema actual que cuenta el hospital.

Según Gálvez (8), en el año 2018 en su tesis titulada “ Implementación de un sistema informático de registro de historias clínicas para el centro de salud de Ricardo Palma - Huarochirí; 2018.” La presente tesis fue desarrollada con una muestra de 12 personas de servicio de admisión y servicio de archivo, la técnica aplicada fue de encuesta, tuvo como resultados que el 66.67 % del personal encuestado expresaron que NO están satisfechos con respecto al sistema actual, con respecto a la segunda dimensión de la Necesidad de implementar un sistema informático de registro de historias clínicas, se pudo observar que el 91.67 % SI tienen la necesidad de implementar un sistema Informático, Según los resultados obtenidos, analizados e interpretados, se concluyen existe la necesidad de implementar el sistema informático que satisfagan las necesidades de la institución debido a la insatisfacción del personal de los servicios de admisión y archivos.

Según Merino (9), en el año 2021 en su tesis titulada " Implementación de un plan de seguridad informática con la norma ISO/IEC 27001 en la empresa Ransa Comercial S.A - Piura; 2021.", se trabajó con una muestra de 27 personas, se utilizó las metodologías MAGERIT, CRAMM y OCTAVE, el 60.00% de los trabajadores encuestados NO están satisfechos con el sistema actual, mientras que el 40.00% indicaron que SI, en relación a la segunda dimensión, se observó que el 80.00% de los encuestados sostienen que SI creen necesario de una nueva propuesta, mientras que el 20% indicaron que NO, esta investigación tiene como alcance resguardar la confidencialidad de los activos de información en la empresa, se concluyó la implementación de un plan de seguridad informática en la empresa Ransa Comercial S.A, mejoró la seguridad de información de sus clientes.

2.2 Bases teóricas

2.2.1 Juzgado de paz de única nominación Canchaque

Reseña Histórica

El 09 de enero del 2017, por medio de la ley número 29824 – Ley de Justicia de Paz, Resolución Nro. 098-2012, que aprueba el Reglamento de elección popular de Jueces de Paz e informe Nro. 001-2017-ODAJUP-csjpi-pj, emitido por la responsable de la oficina Distrital de apoyo a la justicia de paz de la corte superior de Piura.

Ubicación

El despacho del juzgado de paz de única nominación de Canchaque está ubicado en el distrito de Canchaque el cual se sitúa 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, con referencia calle Mishahuaca, Nro. 113.

Objetivo Organizacional

Alcanzar resultados esperados en la visión, misión y funcionales de su ámbito jurídico o geográfico cumpliendo las políticas, leyes y normas.

Visión

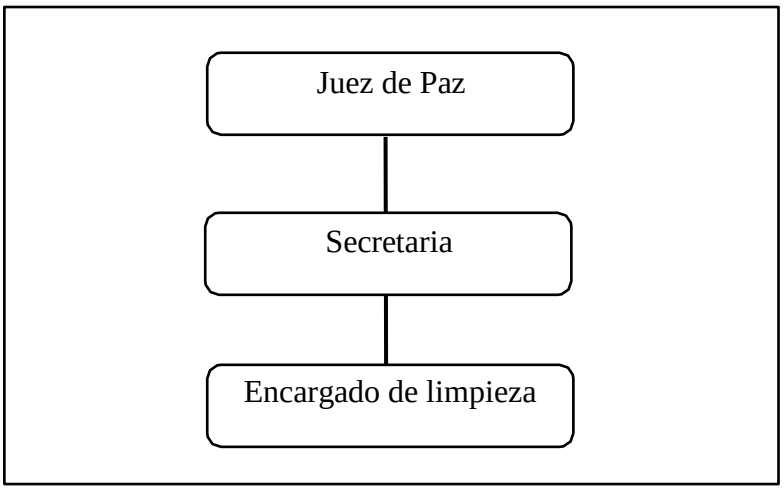
Institución eficiente y autónoma, integrada por Servidores con vocación de servicio comprometidos en lograr la excelencia y Magistrados, que privilegie la solución de conflictos, el acceso oportuno y en condiciones de igualdad a la justicia, respetando los derechos de las personas, contando para ello con un adecuado soporte administrativo y tecnológico.

Misión

"Administrar justicia con equidad y transparencia a través de sus órganos jurisdiccionales, con arreglo a la constitución y a las leyes, garantizando la seguridad y tutela jurisdiccional, para contribuir al estado de derecho, a la paz social y al desarrollo del país".

Organigrama

Gráfico Nro. 1: Organigrama



Fuente: Organigrama del juzgado de paz (31).

2.2.2 La Seguridad Informática

La disciplina de la seguridad se encarga de proteger los activos de una organización o de un particular; Un activo es cualquier elemento que tiene valor para una organización o sujeto, según el tipo de activo a proteger, estaremos tratan• do de seguridad de la información, seguridad de las TIC o ciberseguridad; en general, la seguridad de la información abarca todo aquello que tiene que ver con la protección de la información, ya sea almacenada o transmitida (30).

Direccionamiento IP

Según Romero (10), en su libro “Seguridad Informática Y Alta Disponibilidad” las direcciones IP permiten que todo equipo de una red se encuentre localizado e identificado. Si en alguna circunstancia un equipo no disponga de una dirección IP, estará no podrá comunicarse con el resto de equipos de la red lógica a la que pertenezca. No siendo suficiente, una vez dada una dirección IP a un equipo lógico, este solo podrá comunicarse o contratarse con aquellos equipos que estén conectados a él, a través de un switch o hub, y se identifiquen a la misma red. Si en algún caso que un equipo desee comunicarse o contactarse con equipos que no pertenezcan a su red lógica será necesario un equipo intermediario, como Gateway. finalmente, será necesario indicar al equipo al menos una dirección IP de algún servidor DNS para que se pueda utilizar nombres de dominio “.pe”, “equipo1.midominio.es", "www.google.com", entre otros, con ello ya no se utilizara una dirección IP a la hora de hacer referencia a un equipo.

Los virus informáticos

Los principales y primordiales conceptos de la seguridad informática, son los virus informáticos, la PC(computadoras), lo único que les dan órdenes son los lo 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 (11).

Explotación de vulnerabilidades

El análisis llevado a cabo nos muestra de potenciales vulnerabilidades las cuales son de forma automatizada u manual usando herramientas como Open VAS, un Pentester puede tomar la decisión de verificar estas vulnerabilidades afectarías en gran magnitud por lo que es un riesgo que no debería correr esta empresa, el hecho realizar la verificación en busca de vulnerabilidades es primordial cuando se utilizan sistemas automatizados para la detección, en lo cual algunos resultados solo son falsos y distraen el proceso, por ejemplo la herramienta Open VAS da varias respuestas y una de ellas es una columna de la calidad de detección Q o D, lo que te digo con esto es aunque se encuentre un riesgo puede que no sea correcto (11).

2.2.3 Las Tecnologías de información y comunicaciones

Según Ayala y Gonzales (12), en su libro titulado “Tecnologías De La Información Y La Comunicación” nos da a conocer que Las TIC se desarrollan a partir de los avances científicos producidos en los ámbitos de la informática y las tele comunicaciones. Es el conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos (texto, imagen, sonido, video), el elemento más representativo de las nuevas tecnologías es el ordenador y más específicamente, Internet. Como indican diferentes autores, Internet supone un salto cualitativo de gran magnitud, cambiando y redefiniendo los modos de conocer y relacionarse del hombre, las TIC están presentes en todos los niveles de

nuestra sociedad actual, son tecnologías que se han convertido en imprescindibles para muchas personas y empresas.

TIC en empresas

Según Andrada (13), en su libro titulado “Nuevas Tecnologías de la Información y la Comunicación/NTICX” Las TIC pasan hoyen día todas las áreas de las actividades humanas. El alto avance logrado por la Web 2.0 propone “paradigma de la red”: el trueque de datos digitales, que entrañan la posibilidad de volver a ser nuevamente usados continuamente y poseen la capacidad de circulación, reemplazando hoy en día al tradicional intercambio de objetos o información, como ya sabemos en qué lo único permanente es el trueque (cambio); la sociedad de conocimientos muestra una ventana revolucionaria de la información, que no es tecnológica. No se e aumentar la velocidad de los dispositivos o de nuevo software o de nuevas máquinas. Es una nueva revolución de los conceptos, que plantean sobre la nueva relación del tiempo y el espacio, dimensiones fundamentales de la experiencia humana y que están cambiando por completo las estructuras sociales.

2.2.4 Sistemas de información

Según Hernández (14), en su trabajo de investigación “los sistemas de información: evolución y desarrollo”, los Sistemas de información han ido evolucionando durante los últimos años hasta constituir los denominados sistemas de información estratégicos. Primeramente, los Sistemas de Información empresariales eran considerados como un instrumento simplificador de las distintas actividades de la empresa, una herramienta con la cual se facilitaban los tramites y reducía la burocracia. Su finalidad era básicamente llevar la contabilidad y el procesamiento de los documentos a nivel operativo, posteriormente el desarrollo de la informática y las telecomunicaciones permitieron incrementar la eficacia en la realización de las tareas, ahorrar tiempo en

el desarrollo de las actividades y almacenar la mayor cantidad de información en el menor espacio posible.

2.2.5 Guardar de información

Según López (15) en su libro titulado “Grabación de datos” El proceso de grabación de datos consiste en la transcripción de datos textuales, numéricos o de cualquier otro tipo, utilizando normalmente dispositivos específicos (normalmente equipos informáticos). La finalidad del proceso de grabación de datos es el almacenamiento de los mismos o bien su tratamiento posterior, Los datos transcritos serán suministrados como fuente y será necesario determinar el formato de soporte sobre el cual se realizará la grabación.

2.2.6 Software sin licencia

El software es el componente lógico de cualquier equipo informático que hace la función de intermediario entre el usuario y la computadora. Traduce las órdenes que el usuario le envía mediante los periféricos de entrada (teclado, ratón, etc.) a operaciones que realiza la máquina, para luego mostrar el resultado por los periféricos de salida (por ejemplo, el monitor) (21).

Actualizar sistema operativo

Mantener el SO actualizado es un punto fundamental para el mantenimiento del ordenador. Un equipo desactualizado puede causar problemas con el hardware y con el software que se instale en el mismo. El primer paso para actualizar el SO es identificar cuál es el que se está usando. Este manual se centrará en dos: Windows y Linux (21).

Mantenimiento

Según Romero y otros (11), en su libro titulado “Introducción A La Seguridad Informática Y El Análisis De Vulnerabilidades” en primer lugar, se tiene el propio mantenimiento de los equipos como primordial

instancia y además la aplicación de parches de seguridad, esto no asimila a una magnitud especial, en lo cual se debe tener en cuenta si un riesgo deja de estar presente en ordenadores no será necesario implementar una capa exterior que no de pase a su mal uso.

La administración en la defensa

Según Romero y otros (11), en su libro titulado "Introducción A La Seguridad Informática Y El Análisis De Vulnerabilidades" La dirección de cualquier organización y los principales encargados de administrar cada uno de los departamentos juegan un cargo importante en la seguridad de la infraestructura del uso de la información, para iniciar hay que tener una clara visión, el análisis de riesgos debe efectuarse en gran parte considerando los riesgos no para los equipos, sino para los objetivos de la organización, se trata de saber qué cosas pueden hacer que la organización con la que se trabaje deje de poder cumplir con sus objetivos, sean estos ventas, producción, servicio público o lo que sea, por ello cuando se plantea dar seguridad a los equipos, los líderes de los distintos departamentos deben cooperar tanto en la identificación de riesgos que pueden impedirles cumplir sus funciones como para el desarrollo normal y eficiente del despliegue de medidas técnicas de resiliencia.

2.2.7 Conexiones inalámbricas

Usando la experiencia de cientos de ingenieros de la industria de las comunicaciones, el IEEE a establecido una jerarquía de estándares inalámbricos complementarios. Esto incluye el IEEE 802.15 para Redes de Área Personal (PAN), IEEE 802.11 para Redes de Área Local (LAN), 802.16 para Redes de Área Metropolitana, y el propuesto IEEE 802.20 para Redes de Área Amplia (WAN). Cada estándar brinda una tecnología optimizada para un mercado distintivo, representa un particular modelo de uso y está diseñado para complementarse unos con otros (22).

2.2.8 Internet

Internet se define como una red global de redes de computadoras la cual su finalidad u objetivo es el intercambio o truque de información y datos entre todos los que la usen (usuarios). A veces se malinterpreta su significado como una red de ordenadores. Se puede considerar los ordenadores como el medio de transferencia de los datos e información (23).

2.2.9 Informática

Cernuda y otros (24), en su libro titulado "Informática General" nos dicen que Computación de la República Argentina y la asociación de "docentes de Informática", han acordado en la definición o definiéndola como: La informática es la campo o disciplina de estudio el cual acoge un grupo de saberes (conocimientos), técnicas de tratamiento informático y métodos informáticos de la información, más sus aplicaciones prácticas y teorías, con el único propósito de guardar, procesar y transmitir datos e información en el único formato digital que utilizando sistemas computacionales.

2.2.10 Seguridad de información

Costas (25), en el 2015 en su libro titulado "Seguridad informática" nos habla que la seguridad informática es la que se encarga de asegurarse o verificar los recursos del sistema de información estén siendo manipulados o procesados por la forma en la que se les ordeno correctamente como son los programas (software), así también la información contenida en ellos este siendo distribuida e forma correcta y que no hayan alteraciones o modificaciones que alguien no realizo sin un permiso, nos referimos a las personas acreditadas o autorizadas por el ambiente laboral.

2.2.11 Sistemas operativos

Raya en su libro titulado “Implantación de sistemas operativos” nos dice que el sistema operativo es de por si un programa (software) pero muy especial ya que este es el más complejo e importante cuando es conectado a un ordenador el sistema operativo se almacena en la memoria de este y se ejecuta cada vez que se prende el ordenador en otras palabras es el sistema operativo levanta al PC y realiza el reconocimiento de CPU, las memorias RAM, los Discos de almacenamiento, el teclado, el monitor, la impresora, entre otros y el cual revisa que no sucedan errores de conexión y que los dispositivos sean reconocidos y realicen su función como debe ser, a el primer diagnóstico se le conoce como POST (26).

2.2.12 Seguridad en los Sistemas Operativos

David en su informe de adscripción titulado “Seguridad en los Sistemas Operativos” nos dice que hay riesgos los cuales presentar ser una amenaza clara, son los software maliciosos cono los virus o troyanos hasta el momento los más conocidos son los archivos ejecutables con extensiones como “.com”, “.bat”, “exe” y otros más componentes de Microsoft Office que permiten integrados de macros que traen con si el lenguaje de código abierto Visual Basic para Aplicaciones, básicamente Excel Word y con macros. Los softwares maliciosos como los troyanos se extienden por lo antes mencionado ya que es así su única forma de propagarse siendo archivos ejecutables. Por lo que la única forma de que un troyano se instale en tu ordenador o equipo es (27):

- Haciendo uno mismo el proceso de ejecutarlo a cualquier software o programa infectado, ya sea mediante un diskette, una descarga de internet o abierto desde un “attach” recepcionado por correo electrónico.

- Abriendo un documento de MS-Office 97 o una versión posterior, teniendo deshabilitada o no haciendo caso a la alerta contra macro virus habilitada por defecto en el mismo Office.

2.2.13 Metodología MAGERIT

MAGERIT persigue los siguientes objetivos (28):

1. Concientizar a los encargados de las organizaciones de información de la necesidad de gestionarlos y de la existencia de riesgos.
2. Dar un método sistemático para analizar los riesgos derivados del uso de las TIC (tecnologías de la información y comunicaciones).
3. Ayudar a descubrir y planificar el proceso oportuno para mantener los riesgos controlados indirectamente.
4. La Organización tenerla preparada para procesos de auditoría, acreditación, evaluación y certificación, según sea el caso.

También se ha indagado la uniformidad a los informes que recolectan los hallazgos y las conclusiones de las actividades de gestión y análisis de riesgos (28):

- Modelo de valor

  Caracterización del valor que representan los activos para la Organización, así como de las dependencias entre los diferentes activos.

- Mapa de riesgos

  Concordancia o relación de las amenazas a las que están expuestos los activos.

- Declaración de aplicabilidad

  Para un grupo de salvaguardas, se indica sin son de aplicación en el sistema de información.

- Evaluación de salvaguardas

  Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que debaten.

- Estado de riesgo

  Caracterización de los activos por su riesgo residual; ejemplo, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.

- Informe de insuficiencias

  Debilidad o Ausencia de las salvaguardas que aparecen oportunas para reducir los riesgos sobre el mecanismo o sistema. Ejemplo, recolecta las vulnerabilidades del sistema, entendidas como puntos débilmente protegidos por los que las amenazas podrían materializarse.

- Cumplimiento de normativa

  Satisfacción de unos requisitos, declaración de que se adhiere y es allegado a la normativa correspondiente.

- Plan de seguridad

  Conjunto de proyectos de seguridad que materializan las decisiones de tratamiento de riesgos.

III. HIPÓTESIS

3.1 Hipótesis general

Implementar un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura; 2021, mejora el control de datos e información.

3.2 Hipótesis específicas

1. La determinación del nivel de conocimiento acerca de la seguridad informática del juzgado de paz de única nominación, nos permite conocer las necesidades reales de los colaboradores del juzgado.
2. El análisis a la seguridad información del juzgado de paz de única nominación, le muestra un historial sobre los activos.
3. La implementación de un plan de mejora de seguridad informática en el juzgado de paz de única nominación, le da el acceso a la lista de riegos y amenazas.

IV. METODOLOGÍA

4.1 Diseño de la investigación

El diseño implementado en esta investigación, fue no experimental de corte transversal, porque se apreciaron los eventos tal y como sucedieron y luego fueron analizados.

El tipo de metodología que se utilizó en el desarrollo la investigación fue de tipo cuantitativa nivel descriptivo y de diseño no experimental de corte trasversal.

Este tipo de investigación es más empleada para detallar las características de una población. No confundamos esta descripción con la respuesta a las causas de los fenómenos, también no tiene que detallar la causa de una situación una situación, entonces esto no puede relacionarse como base de una causal donde una variable afecta a otra. Por esto siempre tiene mínimo requerimiento de la validez interna (17).

Mejía (16), el trabajo de investigación cuantitativa es porque en ella se recopilan o recogen y analizan visualizan datos cuantitativos sobre variables de estudio.

4.2 Población y Muestra

Pazmiño (19), en concreto, la muestra constituye y abarca un subgrupo el cual representa el universo y esta representación es una sugerencia ya hemos hablado que la muestra mantiene las característica sus detalles especiales del universo y posteriormente o consiguiente nosotros podamos ampliar los resultados recogidos en el estudio de la muestra a todo el universo, lo cual tiene que tener que los elementos de la fracción sean escogidos aleatoriamente, para garantizar y salvaguardar que dichos elementos tengan la misma posibilidad de ser escogidos.

La población de mi proyecto de investigación consta de una población de 7757 personas de Canchaque, pero mí muestra se tomó por conveniencia escoger a 20 personas las cuales 3 son trabajadores del juzgado y 17 habitantes que frecuentan en el despacho los cuales cumplen los requisitos de atención en el juzgado más de 10, este tipo de investigación es no probabilística.

4.3 Definición operacional de las variables en estudio

Tabla Nro. 1: Definición Operacional

Variable	Definición conceptual	Dimensiones	Indicadores	Definición Operacional
IMPLEMENTACIÓN DE UN PLAN DE SEGURIDAD INFORMÁTICO	La implementación de seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las	Nivel de satisfacción de la implementación de un plan de seguridad informático.	-Tiempo -Administración -Seguridad de información -Uso de dispositivos de PC	SI = 1 NO = 0
		Nivel de conocimiento con respecto al uso de las herramientas TIC	-Seguridad al pasar, modificar o borrar datos	

	personas que se encuentren acreditadas y dentro de los límites de su autorización (20).		-Trabajadores satisfechos -Transmisión de archivos	

Fuente: Elaboración propia

4.4 Técnicas e instrumentos de Recolección de Datos

El presente trabajo de investigación se utilizó como técnica la encuesta y para el instrumento se utilizó un cuestionario de tipo cerrado dicotómico el cual solo cuenta con dos opciones, sí y no.

Una encuesta es un método de recolección de datos obtenidos a través de consultas, cuyo propósito es conocer la opinión de las personas sobre un tema u obtener más información sobre un hecho o evento (32).

4.5 Plan de Análisis

Como primer punto eh analizado el por qué a veces los procesos de tramite no son seguros informáticamente, como segundo punto comprobé si el software tiene licencia, para una mejor atención a los habitantes y trabajadores, además realice la lista del parque tecnológico con él cuenta el juzgado; con los datos obtenidos y listos implemente el plan de seguridad informático el cual aumento la seguridad y también previene riesgos en el juzgado.

En este proceso realice encuetas y para luego tabularlas en excel para poder obtener gráficos y porcentajes los fueron organizados en los resultados con sus respectivos gráficos y cuadros sobre las variables de estudio.

4.6 Matriz de Consistencia

Tabla Nro. 2: Cuadro de consistencia

PROBLEMA	**OBJETIVOS**	**HIPÓTESIS**	**METOLOGÍA**
¿La implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura mejora el control de datos e información?	OBJETIVO GENERAL Implementar un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura; 2021, para mejorar el control de datos e información. Objetivos específicos 1. Evaluar la situación actual de la seguridad informática en el Juzgado de Paz de Única	HIPÓTESIS GENERAL La implementar un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura; 2021, mejorará el control de datos e información. Hipótesis específicas 1. La determinación del nivel de conocimiento acerca de la seguridad informática del	Tipo: Cuantitativo Nivel: Descriptiva Diseño: No experimental de corte trasversal. Universo: 7757 personas Muestra: 20 Personas

	nominación del distrito de Canchaque. 2. Determinar el nivel de conocimiento acerca de la seguridad informática actual del juzgado de paz de única nominación. 3. Implementar un plan de mejora de seguridad informática en el juzgado de paz de única nominación.	juzgado de paz de única nominación, nos permite conocer las necesidades reales de los colaboradores del juzgado. 2. El análisis a la seguridad información del juzgado de paz de única nominación, le muestra un historial sobre los activos. 3. La implementación de un plan de mejora de seguridad informática en el juzgado de paz de única nominación, le da el acceso a la lista de riegos y amenazas.	

4.7 Principios Éticos

Durante el desarrollo de la presente investigación denominada “Implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura, 2021.”, Se ha tenido en cuenta el código de ética de la universidad Católica Los Ángeles de Chimbote, el cual tiene por objetivo plantar los principios y valores éticos, de la misma forma del reglamento de sanción por infracción al ejercicio de la investigación Científica y se ha considerado en forma estricta el cumplimiento de los principios éticos que permitan asegurar la originalidad de la Investigación (33).

Protección de la persona, ya que es primordial cuidar y asegurar la dignidad, creencia y religión, privacidad, confidencialidad, diversidad socio cultural e identidad, también la libre participación y derecho a estar informado esto implica que los ciudadanos se integren en las actividades de investigación por lo que tienen el derecho y la plenitud a estar informados sobre los fines de la investigación y sus propósitos, y respetando los derechos intelectuales de autor.

Principios de beneficencia y no maleficencia, la presente investigación está en balance riesgo-beneficio positivo y justificado, así para asegura el no causar daño, repotencia los beneficios y reduce los efectos negativos.

Principio de justicia, esta investigación vela por poner en primer lugar el bien común antes que el interés personal, y no dar lugar a malas prácticas como la injusticia que se refleja en varios ámbitos de la sociedad.

Principio de integridad científica, aseguramos en poner en claro todos los beneficios potenciales, riesgos y daños que afecten a nuestros participantes de la investigación.

Consentimiento informado y expreso, a todos los encuestados se les brindo la libertad de brindarnos sus datos con un consentimiento informado, para poder realizar nuestro proyecto de investigación.

V. RESULTADOS

5.1 Resultados

Primera Dimensión: Nivel de satisfacción de la implementación de un plan de seguridad informático.

Tabla Nro. 3: Nivel de satisfacción de la implementación de un plan de seguridad informático

Frecuencias de distribución y respuestas allegadas al nivel de satisfacción de la implementación de un plan de seguridad informático. sobre, la implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura, 2021.

Alternativa	n	%
Si	18	90.00
No	02	10.00
Total	20	100.00

Fuente: Cuestionario aplicado a trabajadores y usuarios que frecuentan al Juzgado de paz de única nominación del Distrito de Canchaque, respecto a la pregunta ¿Cree usted que si implantamos un plan de seguridad informático ahorraría tiempo en ejecutar cada proceso?

Aplicado por: Cutin A, 2021.

En la Tabla Nro. 3, se observa que el 90.00% de los encuestados sostienen que, Si implantamos un plan de seguridad informático ahorrarían tiempo en ejecutar cada proceso mientras que el 10.00% piensa que No.

Tabla Nro. 4: Nivel de satisfacción de la implementación de un plan de seguridad informático

Frecuencias de distribución y respuestas allegadas al nivel de satisfacción de la implementación de un plan de seguridad informático. sobre, la implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura, 2021.

Alternativa	n	%
Si	19	95.00
No	1	05.00
Total	20	100.00

Fuente: Cuestionario aplicado a trabajadores y usuarios que frecuentan al Juzgado de paz de única nominación del Distrito de Canchaque, respecto a la pregunta ¿Cree que el plan de seguridad informático ayude a mejorar la administración de los documentos?

Aplicado por: Cutin A, 2021.

En la Tabla Nro. 4, se observa que el 95.00% de los encuestados sostienen que el plan de seguridad informático, Si ayuda a mejorar la administración de documentos y el 05.00% dice que No.

Tabla Nro. 5: Nivel de satisfacción de la implementación de un plan de seguridad informático

Frecuencias de distribución y respuestas allegadas al nivel de satisfacción de la implementación de un plan de seguridad informático. sobre, la implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura, 2021.

Alternativa	n	%
Si	20	100.00
No	-	-
Total	20	100.00

Fuente: Cuestionario aplicado a trabajadores y usuarios que frecuentan al Juzgado de paz de única nominación del Distrito de Canchaque, respecto a la pregunta ¿Cree Usted que capacitaciones sobre seguridad informática serian de relevante importancia para los trabajadores de este juzgado?

Aplicado por: Cutin A, 2021.

En la Tabla Nro. 5, se observa que el 100.00% de los encuestados Si cree que las capacitaciones sobre seguridad informática son de gran relevancia en el juzgado.

Tabla Nro. 6: Nivel de satisfacción de la implementación de un plan de seguridad informático

Frecuencias de distribución y respuestas allegadas al nivel de satisfacción de la implementación de un plan de seguridad informático. sobre, la implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura, 2021.

Alternativa	n	%
Si	13	65.00
No	7	35.00
Total	20	100.00

Fuente: Cuestionario aplicado a trabajadores y usuarios que frecuentan al Juzgado de paz de única nominación del Distrito de Canchaque, respecto a la pregunta ¿Cree Usted que sería necesario incorporar al juzgado controles de seguridad para el uso de los dispositivos de PC?

Aplicado por: Cutin A, 2021.

En la Tabla Nro. 6, Obtenemos que el 65.00% de los encuestados dice que, Si es necesario aplicar controles de seguridad para el uso de dispositivos en la PC, mientras que el 35.00% sostienen que No es necesario.

Tabla Nro. 7: Nivel de satisfacción de la implementación de un plan de seguridad informático

Frecuencias de distribución y respuestas allegadas al nivel de satisfacción de la implementación de un plan de seguridad informático. sobre, la implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura, 2021.

Alternativa	n	%
Si	19	95.00
No	1	05.00
Total	20	100.00

Fuente: Cuestionario aplicado a trabajadores y usuarios que frecuentan al Juzgado de paz de única nominación del Distrito de Canchaque, respecto a la pregunta ¿En el Juzgado ha ocurrido algún hecho referente a la seguridad informática?

Aplicado por: Cutin A, 2021.

En la Tabla Nro. 7, se observa que el 95.00% de los encuestados sostienen que en el juzgado de paz Si ha ocurrido algún incidente referido a la seguridad informática mientras el 05.00% nos informa que No.

Tabla Nro. 8: Nivel de satisfacción de la implementación de un plan de seguridad informático

Frecuencias de distribución y respuestas allegadas al nivel de satisfacción de la implementación de un plan de seguridad informático. sobre, la implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura, 2021.

Alternativa	n	%
Si	20	100.00
No	-	-
Total	20	100.00

Fuente: Cuestionario aplicado a trabajadores y usuarios que frecuentan al Juzgado de paz de única nominación del Distrito de Canchaque, respecto a la pregunta ¿Cree que es necesario aplicar un plan de seguridad informático en el Juzgado?

Aplicado por: Cutin A, 2021.

En la Tabla Nro. 8, obtenemos que el 100.00% de los encuestados nos informa que Si es necesario aplicar el plan de seguridad informática el juzgado de paz.

Resumen de la dimensión nivel de satisfacción de la implementación de un plan de seguridad informático

Tabla Nro. 9: Resumen de la primera dimensión

Nivel de satisfacción de la implementación de un plan de seguridad informático. sobre, la implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura, 2021.

Alternativa	n	%
Si	20	100.00
No	-	-
Total	20	100.00

Fuente: Cuestionario aplicado a trabajadores y usuarios que frecuentan al Juzgado de paz de única nominación del Distrito de Canchaque.

Aplicado por: Cutin A, 2021.

En la Tabla Nro. 9, obtenemos que el 100.00% de los encuestados nos informa que Si es necesario implementar el plan de seguridad informática el juzgado de paz.

Segunda Dimensión: Nivel de conocimiento con respecto al uso de las herramientas TIC

Tabla Nro. 10: Nivel de conocimiento con respecto al uso de las herramientas TIC.

Frecuencias de distribución y respuestas allegadas al nivel de satisfacción de la implementación de un plan de seguridad informático. sobre, la implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura, 2021.

Alternativa	n	%
Si	13	35.00
No	7	65.00
Total	20	100.00

Fuente: Cuestionario aplicado a trabajadores y usuarios que frecuentan al Juzgado de paz de única nominación del Distrito de Canchaque, respecto a la pregunta ¿Usted sabe la importancia del mal manejo de la información?

Aplicado por: Cutin A, 2021.

En la Tabla Nro. 10, se observa que el 65.00% de los encuestados sostiene que, No sabe la importancia del mal manejo de la información, mientras que el 35.00% Si.

Tabla Nro. 11: Nivel de conocimiento con respecto al uso de las herramientas TIC

Frecuencias de distribución y respuestas allegadas al nivel de satisfacción de la implementación de un plan de seguridad informático. sobre, la implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura, 2021.

Alternativa	n	%
Si	19	95.00
No	1	05.00
Total	20	100.00

Fuente: Cuestionario aplicado a trabajadores y usuarios que frecuentan al Juzgado de paz de única nominación del Distrito de Canchaque, respecto a la pregunta ¿Usted considera que con un plan de seguridad informática estará más a gusto (seguro) con su trabajo?

Aplicado por: Cutin A, 2021.

En la Tabla Nro. 11, El 95.00% de los encuestados sostiene que Si estaría a gusto con un plan de seguridad informático en el juzgado, y el 05.00% sostiene que No.

Tabla Nro. 12: Nivel de conocimiento con respecto al uso de las herramientas TIC

Frecuencias de distribución y respuestas allegadas al nivel de satisfacción de la implementación de un plan de seguridad informático. sobre, la implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura, 2021.

Alternativa	n	%
Si	9	45.00
No	11	55.00
Total	20	100.00

Fuente: Cuestionario aplicado a trabajadores y usuarios que frecuentan al Juzgado de paz de única nominación del Distrito de Canchaque, respecto a la pregunta ¿Usted considera que el manejo o tratado de archivos es fácil de realizar en una computadora?

Aplicado por: Cutin A, 2021.

En la Tabla Nro. 12, obtenemos que el 55.00% de los encuestados nos dice que el manejo y tratado de archivos en una computadora No es fácil de realizar por lo tanto el 45.00% sostienen que Si.

Tabla Nro. 13: Nivel de conocimiento con respecto al uso de las herramientas TIC

Frecuencias de distribución y respuestas allegadas al nivel de satisfacción de la implementación de un plan de seguridad informático. sobre, la implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura, 2021.

Alternativa	n	%
Si	7	35.00
No	13	65.00
Total	20	100.00

Fuente: Cuestionario aplicado a trabajadores y usuarios que frecuentan al Juzgado de paz de única nominación del Distrito de Canchaque, respecto a la pregunta ¿Usted conoce sobre las herramientas Tecnologías de la información y la comunicación (TIC)?

Aplicado por: Cutin A, 2021.

En la Tabla Nro. 13, Observamos que el 65.00% de los encuestados confirman que No conocen o no tienen conocimiento sobre las herramientas Tecnologías de la información y la comunicación (TIC), mientras que el 35.00% nos dice Si conoce.

Tabla Nro. 14: Nivel de conocimiento con respecto al uso de las herramientas TIC

Frecuencias de distribución y respuestas allegadas al nivel de satisfacción de la implementación de un plan de seguridad informático. sobre, la implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura, 2021.

Alternativa	n	%
Si	-	-
No	20	100.00
Total	20	100.00

Fuente: Cuestionario aplicado a trabajadores y usuarios que frecuentan al Juzgado de paz de única nominación del Distrito de Canchaque, respecto a la pregunta ¿En el Juzgado de Paz realizan capacitaciones sobre seguridad informática?

Aplicado por: Cutin A, 2021.

En la Tabla Nro. 14, Observamos que el 100.00% de los encuestados sostienen que en el Juzgado No se realizan capacitaciones sobre seguridad informática.

Resumen de la segunda dimensión nivel conocimiento con respecto al uso de las herramientas TIC.

Tabla Nro. 15: Resumen de la segunda dimensión

Nivel de conocimiento con respecto al uso de las herramientas TIC. De la implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura, 2021.

Alternativa	n	%
Si	7	35.00
No	13	65.00
Total	20	100.00

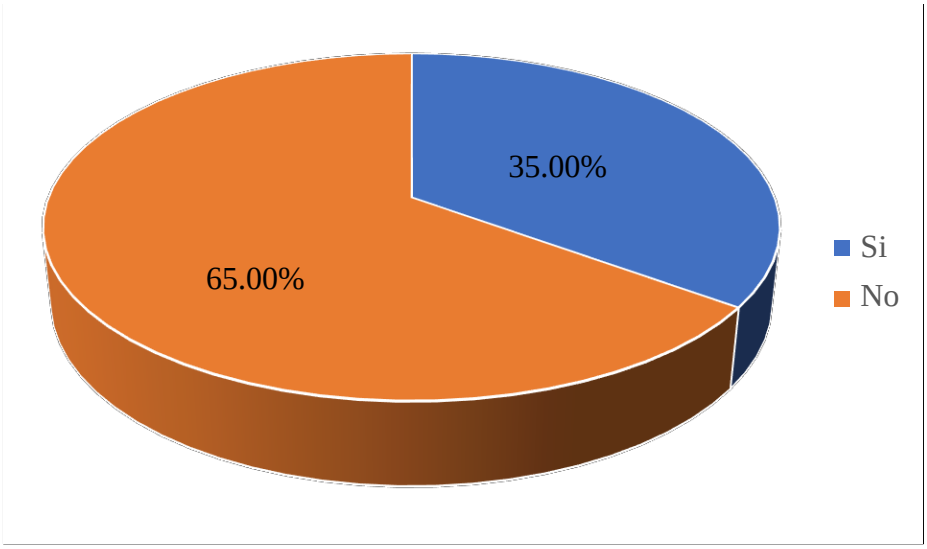
Fuente: Cuestionario aplicado a trabajadores y usuarios que frecuentan al Juzgado de paz de única nominación del Distrito de Canchaque.

Aplicado por: Cutin A, 2021.

En la Tabla Nro. 15, Observamos que el 65.00% de los encuestados afirman que No conocen o no tienen conocimiento sobre las herramientas Tecnologías de la información y la comunicación (TIC), mientras que el 35.00% nos dice Si conoce.

Gráfico Nro. 2: Resumen de la Dimensión sobre el Nivel de conocimiento con respecto al uso de las herramientas TIC

Nivel de conocimiento con respecto al uso de las herramientas TIC. De la implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura, 2021.



Fuente: Ttabla Nro. 15

RESUMEN GENERAL DE LAS DIMENSIONES

Tabla Nro. 16: Resumen general de dimensiones

Distribución de frecuencias de las dimensiones Nro. 01 y 02, en relación a la Implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura, 2021.

	SI		NO		Total	
Nivel de satisfacción	n	%	n	%	n	%
de la implementación de un plan de seguridad informático.	20	100.00	-	-	20	100.00
Resumen de la Dimensión sobre el Nivel de conocimiento con respecto al uso de las herramientas TIC.	7	35.00	13	65.00	20	100.00

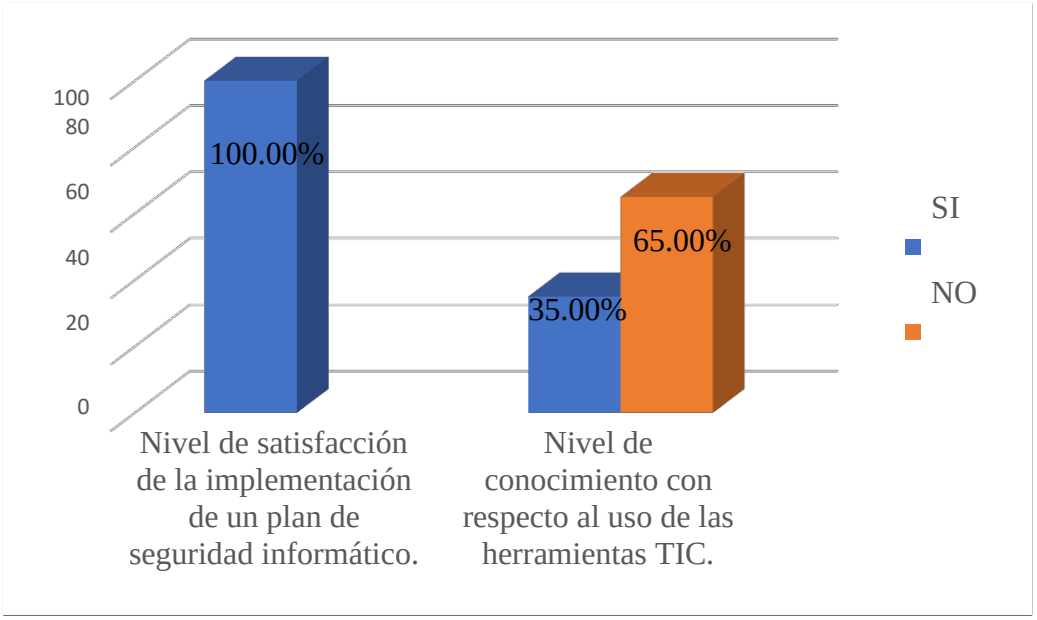
Fuente: Cuestionario aplicado a trabajadores usuarios que frecuentan al Juzgado de paz de única nominación del Distrito de Canchaque – Piura; 2021.

Aplicado por: Cutin A, 2021.

En la Tabla Nro. 16, se observa que el 100.00% de los encuestados Si están conformes con la implementación de un plan de seguridad informático y a su vez el 65.00% de los encuestados No, conocen sobre las herramientas Tic y el 35.00% Si conoce, por lo que es necesario aplicar este plan de seguridad informático.

Gráfico Nro. 3: Resumen General de las Dimensiones

Resumen general de dimensiones, en respecto a la implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura, 2021.



Fuente: Tabla Nro. 15

5.2 **Análisis de resultados**

El objetivo general de esta presente investigación fue: Implementar un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura; 2021, para mejorar el control de datos e información, para solucionar la baja y escasa seguridad informática, que existe en el juzgado de paz de única nominación Canchaque; en ese camino para poder realizar la evaluación de la situación actual con el fin de identificar e interpretar los resultados obtenido para que la propuesta de mejora pueda cumplir con las exigencias encontradas.

Se realizo un cuestionario dividido en 2 dimensiones y aquí el análisis de los resultados e interpretados de las respuestas.

1. Por los resultados obtenidos declaramos que el juzgado de paz de única nominación de Canchaque aprueba este proyecto con un grado de certeza del 100% siendo como resultado principal de la dimensión "Nivel de satisfacción de la implementación de un plan de seguridad informático", este resultado al ser comparado con la tesis de Celis (6), en su tesis titulada "Plan de Seguridad de la Información aplicado a la Central Hidroeléctrica Carhuaquero", los cuales terminaron obteniendo el 100.00% de cumplimiento en la propuesta e implementación y también comparado con la investigación de Solano (7), titulada "Implementación de un sistema informático de hospitalización del hospital Elpidio Berovides Pérez – Otuzco; 2018.", donde encontró que el 100.00% de trabajadores si aprueban la necesidad de implementar un sistema informático de hospitalización. Esto los ayudo para la prevención de la seguridad de la información, por lo que es una luz verde para aplicar el objetivo general de implementar el plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura; 2021, para mejorar el control de datos e información, el cual será muy beneficioso para el juzgado y su población de 7577 habitantes, además según Romero y otros autores (11), nos menciona en su libro titulado "Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades", nos dice que la seguridad informática encarga de la seguridad del medio informático, según varios autores la informática es la ciencia encargada de los procesos, técnicas y métodos que buscan procesar almacenar,

transmitir la información y también te permite entender donde puedes tener vulnerabilidades en tus sistemas informáticos, para una vez detectadas, tomar las medidas necesarias para prevenir esos problemas.

2. En los resultamos podemos apreciar y fijar que carecen de un poco de conocimiento sobre las tecnologías de la información, ya que los resultados obtenidos de los encuestados fueron de 65.00% No conocían sobre las herramientas Tic y el 35.00% si conocía, al ser comparado con el trabajo de investigación de Gálvez (8), titulado "Implementación De Un Sistema Informático De Registro De Historias Clínicas Para El Centro De Salud De Ricardo Palma - Huarochirí; 2018.", el cual obtuvo un 66.67% de sus encuestados si deseaba un nuevo sistema informático y también tienen una similitud con el trabajo de investigación de Torres (2), titulado "Plan de seguridad informático basado en la norma ISO 27001, para proteger la información y activos de la empresa privada Megaprofer S.A.", donde se logra evidenciar que el 10.00% su conocimiento es bueno, el 40.00% es regular, el
15.00% su conocimiento es muy deficiente y el 35.00% no tiene conocimiento sobre el tema, en otras palabras desean tener un mejor conocimiento sobre el tema, por es fundamental y necesario aplicar este plan de seguridad informático ya que en mi propuesta de mejora eh desarrollado las soluciones para poder elevar este 35.00% de conocimiento sobre las TIC, además Ayala y Gonzales (12), en su libro titulado "Tecnologías de la Información y la comunicación", nos da a conocer que Las TIC se desarrollan a partir de los avances científicos producidos en los ámbitos de la informática y las tele comunicaciones. Es el conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos como video, texto, sonido, imagen, también que son aparatos electrónicos y dispositivos digitales que facilitan el acceso e intercambio de datos e información: ordenadores, smartphones entre otros. Igual las redes inalámbricas por Wifi, apps y software diseñados para optimizar la comunicación, la conexión, desarrollar productividad, entre otras cosas.

5.3 Propuesta de mejora

Como centro importante para esta propuesta, es realizar un análisis de la situación actual, además esta propuesta de mejora esta desarrollada bajo la norma ISO 27001, utilizando la "METODOLOGIA MAGERIT" para brindar el cumplimiento de la seguridad informática con respecto a los riesgos y los activos. E escogido esta metodología porque es fundamental en empresa la seguridad de la información, por lo que se necesita conocer y controlar los riesgos a los cuales está expuesta la información de la compañía. A veces las empresas buscan como implementar modelos de gestión de seguridad de la información, pero suelen utilizar metodologías que las que les ofrezcan un marco de trabajo definido que facilite la administración de los riesgos y además permita mejorarla.

5.3.1 Análisis

Análisis de procesos

En el Juzgado de paz de única nominación del distrito de Canchaque se realizan diversos trámites documentarios, dejando de lado las denuncias por delito ya que esta orden se la quitaría en el año 2022, además cuando realizan sus procesos es demasiado riesgoso en temas de protección a la seguridad informática ya que cuenta con deficiencias en el siguiente listado se encentran los procesos más que se realizan:

- Actas: como competencia del Juez, la redacción de actas de comparendo, contratación, entre otras, todo este proceso se realiza en la PC, y se imprime luego de haber terminado y pone su cello para al final ser entregadas a su destino.
- Constancias: Realiza constancias de posesión, de negocio, entre otras que son competencias del juez de paz de única nominación, la constancia se redacta primero en físico y luego es trascribirlo al ordenar por la secretaria y al final es entregado y firmado entregado a su destino.

- Permisos de viaje: este tipo de documentos son realizados por el juez en la computadora y luego es impreso para ser sellado y firmado y llegue a su destino final.
- Conciliaciones: en las conciliaciones se hacen verbalmente y todo lo que van hablando las parte involucradas es escrito y redactado en el ordenador para al final llegar a un acuerdo, y ser impreso, sellado y entregado a su destino final.

Personal de acceso al PC

- Juez
- Secretarias
- Soporte técnico

Vulnerabilidades

- Software sin licencia
- Uso no adecuado de USB.
- La PC no cuentas con Antivirus
- No conocimiento de la ISO 27001
- No hay registro o protocolo establecido para una incidencia

5.3.2 Matriz FODA

Se realizo el análisis FODA (Matriz) para dar a mostrar oportunidades, fortalezas, debilidades y amenazas que se presentan en el parque informático del juzgado de paz de única nominación de Canchaque de acuerdo a la información que eh recolectado en el trabajo de campo.

Tabla Nro. 17 Matriz FODA

FORTALEZAS	OPORTUNIDADES
Se le hace servicio técnico a la PC cuando le entra virus, se pone lenta o en caso que presente inconveniente. El juez reconoce la falta de seguridad informática en su despacho	Contar con la disposición y el presupuesto para la compra e innovación de las herramientas para tener una mejor seguridad de la información. Otorgar un plan para la mejora en cuanto a la seguridad de la información. Enfoque en la seguridad de la información para posibles amenazas En cuanto a la seguridad de la información dar capacitaciones a todo el personal de la entidad. Implementación de la Norma ISO 27001
DEVILIDADES	AMENAZAS
No cuenta con un Antivirus El personal no cuenta con licencias de software.	El no contar con antivirus brinda una seguridad no optima.

No hay amplio conocimiento sobre la seguridad de la información. El acceso al área de servidores no se encuentra bien protegida. No cuenta con políticas o base estandarizada u fija por si ocurre algún incidente. No existe algún protocolo a seguir si ocurre perdida de información contingencia en caso de pérdida de información. Falta capacitación con respecto a seguridad de la información. Falta de apoyo en el proceso de TICS.	Pérdida de información por no guardar correctamente los documentos. No cuenta con la implementación de firewall, equipos vulnerables en la red. Software sin licencia (paquete de office). Afectación a la integridad de los datos por mar manipulación del parque tecnológico.

Fuente: Elaboración propia

5.3.3 Conclusiones y recomendaciones situación actual del Juzgado

Conclusiones

- El personal de soporte técnico no está presente cuando se necesita, en lo que concierte al juez no tiene un alto conocimiento sobre la seguridad informática, como procedimientos de defensa y protección de datos en el ámbito de información.
- La infraestructura del juzgado se encuentra divida por procesos, gracias a ello se pudo conocer las actividades que se desarrollan dentro de cada una de ellas, se determinan la seguridad en el hardware y software, infraestructura, soporte a usuarios.
- El juzgado anteriormente ha sufrido acontecimientos de perdida de información debido a al desconocimiento y a falta de políticas de seguridad para que sigan una normatividad adecuada, llegando hasta tener problemas en la información, lo cual la lleva a pérdidas de tiempo eh información mal manipulada.
- El despacho de Juzgado es muy trascurrido por los documentos que se realizan a diario, por los pobladores y con este trabajo se ha enfocado en la seguridad de la información con la NORMA ISO 27001 referente a los activos de a información.
- Con los programas sin licencia y sin un antivirus el juzgado está expuesto que su información sea robada, perdida u incluso borrada por el mal uso y por qué está expuesta a Phishing al no tener un Firewall o filtro en su red de navegación por internet.

Recomendaciones

- Implementar el plan de seguridad a todos los activos que sean empleados en la trata de la información como el ordenador, la impresora, entre otros basándose en la NORMA ISO27001 para así generar un control adecuado en los activos.
- Desarrollar lo más pronto posible las políticas y controles adecuados, en base a la normatividad ISO 27001, con el fin de minimizar riesgos en los activos de información y fortalecer la gestión de seguridad en el despacho.

- Elaborar una correcta y buena gestión de riesgos en base a una metodología, la cual ayudará a encontrar amenazas en los activos de información de una manera eficiente para establecer medidas de seguridad y que estas sean capaces de responder ante cualquier incidente.

5.3.4 Implementación SGSI

Basado en la normativa ISO 27001 se presenta el SGSI con la versión del año 2013. Siendo este un modelo sistémico de carácter preventivo en cuanto nos referimos a la seguridad de la información el cual nos brinda integridad, disponibilidad y confidencialidad, para darnos respuesta a los riesgos que se pueden contrarrestar los activos y que estos sean gestionados de la mejor manera correcta posible.

El presente sistema de gestión de seguridad implementada será en las siguientes etapas:

- Definir el alcance, políticas de SGIS y objetivos.
- Identificar los riesgos de los activos definidos en el alcance SGSI
- Analizar las probabilidades e impactos de riesgos sobre los activos que fueron identificados el alcance y así calcular los niveles de riesgo, aplicando la metodología MAGERIT.
- Implementar controles sobre los activos, fijándonos y basándonos en un plan de tratamiento de riesgo.
- Asegurar la creación de procedimientos para el monitoreo y revisión del SGIS.

5.3.5 Alcance

Para fijar el alcance de la implementación del SGSI, nos basaremos en los procesos de la siguiente imagen, ya que todo ello engloba a las actividades que se realizan en el despacho.

Figura Nro. 01: Procesos del Juzgado

Fuente: Elaboración propia

Se deberán evaluar los procesos considerados en el alcance y en cuanto a la norma estándar ISO 27001:

- Tomar en cuenta la gestión de activos fijados, existentes en la organización en base a una gestión más adecuada a los riesgos y que vulnerable se encuentra, así como la gestión de responsabilidades y usos apropiados de los activos.
- Seguridad física, la manipulación de algún recurso físico del juzgado que sea mal utilizado por la secretaria o por un tercero, estos controles deben ser aplicados de manera correcta.
- Gestión de accesos, debido al no tener controles para la gestión de los mismos vendría a ser uno de los factores relevantes para así garantizar la efectividad de continuar la labor de sus actividades, brindando efectividad en todo momento de la información.
- Equipos físicos, aquí aplicar controles que comprendan el mantenimiento preventivo como también correctivo, para brindar un mejor rendimiento eficiente en todos sus ámbitos y así conservar la integridad del Software y Hardware.

El presente alcance ha sido logrado y desarrollado bajo la Norma ISO 27001, ya que con esto llevo a cabo el SGSI que tendrá mucho valor en el área de trabajo del Juzgado para verificar las etapas que se han establecido.

5.3.6 Política de seguridad del SGSI

Para la siguiente implementación del Sistema de Gestión de la Seguridad de la Información (SGSI), se establece la política siguiente, la cual se encuentra alineada con el contexto y ambiente de seguridad de la información y la entidad del juzgado, donde se tiene lugar la implementación del SGSI.

"Impulsar las prácticas de seguridad de la información, con el fin de dar garantía a la calidad y magnificencia en la trata de la información, permitiendo reforzar la continuidad de los procesos del juzgado de paz de única Nominación Canchaque mediante de un Sistema de Gestión de Seguridad de la Información que constituye el marco de referencia para lograr la consecución de este compromiso así fijar la confidencialidad, integridad y disponibilidad de la información."

Objetivos: con el motivo de llevar a cabo la política establecida para el Juzgado se establecen los siguientes objetivos:

- Considerar la seguridad de la información como un proceso de mejora continua, que cada vez de paso a llegar a niveles de seguridad más avanzados y altos para la institución como es el Juzgado de Paz de única nominación.
- Generar la adecuada gestión de riesgos que puedan detectar las vulnerabilidades posibles en los activos de información para ser corregidos de manera exitosa.
- Definir, desarrollar e implementar los controles de seguridad organizativos que resulten necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada en el juzgado de paz de única Nominación Canchaque.

5.3.7 Gestión de riesgos

Para la gestión de los riesgos es importante evaluar el impacto de los mismos que tendrá para la institución, en el cual teniendo en consideración las posibles consecuencias que logren afectar los procesos que se desarrollan en el manejo de la información.

El propósito de este paso es decidir si el riesgo es aceptable o de lo contrario buscar y aplicar un método adecuado para contrarrestarlo o mitigarlo.

Para la ejecución de esta sección, se ha definido una metodología con la cual se realizará el análisis y evaluación de riesgos. El método consiste en un análisis cualitativo de los activos más relevantes que pertenecen a al ambiente del juzgado, siguiente la identificación de las amenazas (riesgos) relacionadas con ellos y su probabilidad de ocurrencia; en base a esto, se describen las vulnerabilidades que podrían hacer que dichas amenazas se cumplan.

A continuación, se muestra un diagrama de la metodología a utilizar:

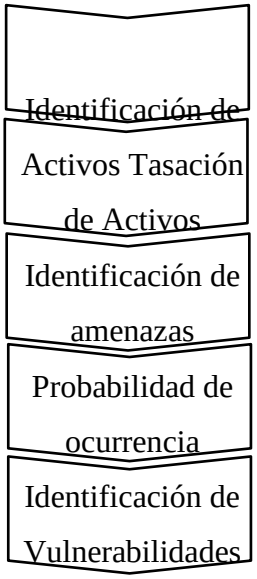


Fig. N° 02: Metodología de riesgos
Fuente: Elaboración propia

- Identificación de activos: Todos los activos que la empresa dispone, tienen un mucho valor significativo porque trabaja con la información, por lo tanto, es primordial proporcionar una protección adecuada.

  Después de identificar todos los activos, se los evalúa para administrar aquellos que se consideran "más relevantes".

- Al tener identificado los activos considerados de "mayor relevancia", se determinan las vulnerabilidades como las amenazas, luego de eso se determina el nivel de impacto en los activos del Juzgado.
- Procedemos a determinar y evaluar la probabilidad real de ocurrencia de dicha amenaza, teniendo en cuenta las consecuencias y el impacto que tendrán si llegan a cumplirse, lo es un riesgo relacionado con la integridad, confidencialidad y disponibilidad de la información.
- Finalmente, el valor de riesgo se obtiene en la tabla establecida para verificar la frecuencia de ocurrencia de la amenaza.

Inventario de activos informáticos

Para llegar al objetivo planteado que es la implementación del SGSI es importante cumplir con el análisis y la gestión de riesgos de los activos vinculados a la información, que la empresa dispone para los procesos que realiza.

METODOLOGIA MAGERIT

El uso de esta metodológica es infalible ya que su enfoque es a los activos más importantes de la empresa y a todos aquello que se relacionan con los activos de información.

Para un mejor análisis, se va a trabajar por agrupar los activos acordes con la metodología MAGERIT la se centra la gestión de los riesgos.

Tabla Nro. 18: Riesgos MAGERIT (tipos de activos)

Activos	Descripción
Instalaciones [L]	Lugares donde se hospedan los sistemas de información y comunicaciones.
Hardware [HW]	Los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización
Software [SW]	Tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de servicios.
Redes de comunicaciones [COM]	Son los medios de transporte que llevan datos de un sitio a otro. Se incluyen tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros.
Equipamiento Auxiliar [AUX]	Otros equipos que sirven de soporte a los sistemas de información, sin

	estar directamente relacionados con éstos.
Personal [P]	Personas relacionadas con los sistemas de información.
Soportes de información [M]	Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

Fuente: Elaboración propia

Tabla Nro. 19: Identificación de Activos Informáticos

TIPO DE ACTIVO	ID	ACTIVO
INSTALACIONES [L]	L1	Instalaciones generales
	L2	Seguridad Física
	L3	Recepción
HARDWARE [HW]	HW1	Computadores de Escritorio
	HW2	Impresoras
	HW3	Router
	HW4	Estabilizador
SOFTWARE [SW]	SW1	Microsoft Office
	SW2	Sistema Operativo Windows
	SW3	Antivirus
REDES DE COMUNICACIÓN [COM]	COM1	Acceso a Internet
EQUIPAMIENTO AUXILIAR	AUXI	Sistema Eléctrico
PERSONAL [P]	P1	Juez

	P2	Secretaria
SOPORTES DE INFORMACION [M]	M1	Discos Solido
	M2	USB

Fuente: Elaboración propia

Para identificar los riesgos en los activos de información, cada uno de los activos se evalúa de acuerdo con el nivel de Confidencialidad, Disponibilidad e Integridad que proporcionan para garantizar la información en un rango entre 1 a 5 llevados a cabo, donde se detallan los siguientes niveles:

Tabla Nro. 20 Niveles de Riesgo

Niveles (C, D, I)	ID
Extrema	5
Alta	4
Media	3
Baja	2
Muy Baja	1

Fuente: Elaboración propia

Tabla Nro. 21 Identificación de riegos

ACTIVO	Confidencialidad	Disponibilidad	Integridad	Total
Instalaciones generales	3	3	2	3
Seguridad Física	4	4	4	4
Recepción	1	1	2	1
Computadores de Escritorio	4	4	3	4
Impresoras	4	3	2	3
Router	4	4	3	4
Estabilizador	4	4	3	4

Microsoft Office	3	4	3	3
Sistema Operativo Windows	4	4	3	4
Antivirus	3	4	3	3
Acceso a Internet	5	5	3	4
Sistema Eléctrico	4	4	3	4
Juez	3	2	2	2
Secretaria	2	3	2	2

Fuente: Elaboración propia

Luego de la tabla anterior se organizan en una lista cuyos activos sean mayores o iguales a 3 para realizar la evaluación de riesgos.

Tabla Nro. 22 Identificación de riegos

ACTIVO	Total
Instalaciones generales	3
Seguridad Física	4
Computadores de Escritorio	4
Impresoras	3
Router	4
Estabilizador	4
Microsoft Office	3
Sistema Operativo Windows	4
Acceso a Internet	4
Sistema Eléctrico	4

Fuente: Elaboración propia.

Tabla Nro. 23 Catálogo de amenazas según MAGERIT

Tipo de Activo	ID	Amenazas
Desastres Naturales [N]	N1	Fuego
	N2	Daños por agua
	N3	Tormenta Eléctrica
	N4	Terremoto
Origen Industrial [I]	I1	Fuego
	I2	Daños por agua
	I3	Sobrecarga eléctrica
	I4	Explosión
	I5	Derrumbe
	I6	Contaminación Mecánica
	I7	Contaminación electromagnética
	I8	Avería de origen física o lógica
	I9	Corte eléctrico
	I10	Condiciones inadecuadas de temperatura Y/O humedad
	I11	Fallo del servicio de comunicaciones
	I12	Interrupciones de otros servicios y suministros esenciales
	I13	Degradación de los soportes de almacenamiento de información
	I14	Emanaciones Electromagnéticas
Errores y fallos no intencionados [E]	E1	Errores de usuarios
	E2	Errores de los técnicos de TI
	E3	Errores de los administradores de sitio
	E4	Errores de monitorización (log)
	E5	Errores de configuración
	E6	Deficiencias en la organización
	E7	Difusión de software dañino

	E8	Errores de [re-]encaminamiento
	E9	Errores de secuencia
	E10	Escapes de información
	E11	Alteración accidental de la información
	E12	Destrucción de información
	E13	Fugas de información
	E14	Vulnerabilidad de los programas (software)
	E15	Errores de mantenimiento / actualización de programas (software)
	E16	Errores de mantenimiento / actualización de equipos (hardware)
	E17	Caída del sistema por agotamiento de recursos
	E18	Pérdida de equipos
	E19	Indisponibilidad del personal
Ataques intencionados [A]	A1	Manipulación de los registros de actividad (log)
	A2	Manipulación de la configuración
	A3	Suplantación de la identidad del usuario
	A4	Abuso de privilegios de acceso
	A5	Uso no previsto
	A6	Difusión de software dañino
	A7	[Re-]encaminamiento de mensajes
	A8	Alteración de secuencia
	A9	Acceso no autorizado
	A10	Análisis de tráfico
	A11	Repudio
	A12	Interceptación de información (escucha)
	A13	Modificación deliberada de la información

	A14	Destrucción de información
	A15	Divulgación de información
	A16	Manipulación de programas
	A17	Manipulación de los equipos
	A18	Denegación de servicio
	A19	Robo
	A20	Ataque destructivo
	A21	Ocupación enemiga
	A22	Indisponibilidad del personal
	A23	Extorsión
	A24	Ingeniería social

Fuente: Elaboración Propia

Para poder estimar la frecuencia de la vulnerabilidad se necesita ver la ocurrencia de amenazas en una escala de tiempo.

Tabla Nro. 24 Categoría de fuentes de amenaza

Vulnerabilidad	ID	Rango
Extrema Frecuencia	MA	1 vez al día
Alta Frecuencia	A	1 vez cada 2 semanas
Frecuencia Media	M	1 vez cada 2 meses
Baja Frecuencia	B	1 vez cada 6 meses
Muy Baja Frecuencia	MB	1 vez al año

Fuente: Elaboración propia

Para la valoración del impacto con respecto a la frecuencia de una amenaza se basará en la siguiente tabla y así determinar un valor en las dimensiones aplicadas:

Tabla Nro. 25 Valoración del impacto de amenaza

Impacto	ID	Valor
Muy Alto	MA	Valor > 95%
Alto	A	75%<Valor>95%
Medio	M	50%<Valor>75%
Bajo	B	30%<Valor>50%
Muy Bajo	MB	10%<Valor>30%

Fuente: Elaboración propia

Continuando, mostramos la tabla de resumen del análisis de amenazas del Juzgado de paz de única nominación Canchaque, se visualiza que cada amenaza afecta un activo, se analiza la frecuencia de ocurrir este suceso y su impacto de seguridad del activo.

Tabla Nro. 26 Análisis de amenazas

Grupo	Amenaza	Activo Afectado	Frecuencia	% Impacto – Dimensiones		
				C	D	I
Desastres Naturales	Fuego	INSTALACIONES [L]	MB		100	100
		REDES DE COMUNICACIÓN [COM]	MB		75	75
		EQUIPAMIENTO AUXILIAR	MB		75	75
	Daños por agua	INSTALACIONES [L]	MB		100	100
		HARDWARE [HW]	MB		100	100

		REDES DE COMUNICACIÓN [COM]	B		100	100
	Corte eléctrico	REDES DE COMUNICACIÓN [COM]	M		100	100
	Terremoto	INSTALACIONES [L]	MB		100	100
		HARDWARE [HW]	MB		100	100
		SOFTWARE [SW]	MB		100	100
		REDES DE COMUNICACIÓN [COM]	MB		50	50
		EQUIPAMIENTO AUXILIAR	MB		50	50
		PERSONAL [P]	MB		75	75
		SOPORTES DE INFORMACION [M]	MB		100	100
	Condiciones inadecuadas de temperatura Y/O humedad	INSTALACIONES [L]	B		100	100
		HARDWARE [HW]	MB		100	100
		SOFTWARE [SW]	MB		100	100
		REDES DE COMUNICACIÓN [COM]	MB		100	100
	Fallo del servicio de comunicaciones	REDES DE COMUNICACIÓN [COM]	B		100	100

	Degradación de los soportes de almacenamiento de información	SOPORTES DE INFORMACION [M]	MB		100	100
	Errores de usuarios	PERSONAL [P]	B		100	100
	Errores de los técnicos de TI	INSTALACIONES [L]	MB		100	100
		HARDWARE [HW]	MB		100	100
		SOFTWARE [SW]	MB		100	100
		REDES DE COMUNICACIÓN [COM]	MB		50	50
	Difusión de software dañino	SOFTWARE [SW]	M		100	100

Fuente: Elaboración propia

Después que se realizó la evaluación y el análisis de riesgos de los activos principales en el Juzgado de Paz, se identificó las probabilidades de amenaza y ocurrencia se puede decir que fueron los activos con más probabilidad de ocurrir una incidencia, ya sea por fallos, el clima, u la propia naturaleza, entre otros.

Para culminar con la implementación del SGSI se aplica los siguientes puntos de recomendación de la NORMA ISO 27001:

- El Juez de Paz puede solicitar a la municipalidad del distrito productos para innovar o servicios tecnológicos que concuerden con los procesos del Juzgado de Paz.
- Establecer procedimientos de la documentación para el anexado del inventario de todos los archivos en físico con los que cuenta ya que están expuestos a muchos riesgos.

- Solicitar apoyo a la municipalidad sobre charlas o capacitaciones al personal que labora sobre correcto uso de los equipos tecnológicos del Juzgado de Paz.
- Fijar una política de sanciones por uso inadecuado o alguna falta indebida en la información o servicio TI.

5.3.8 Presupuesto Económico

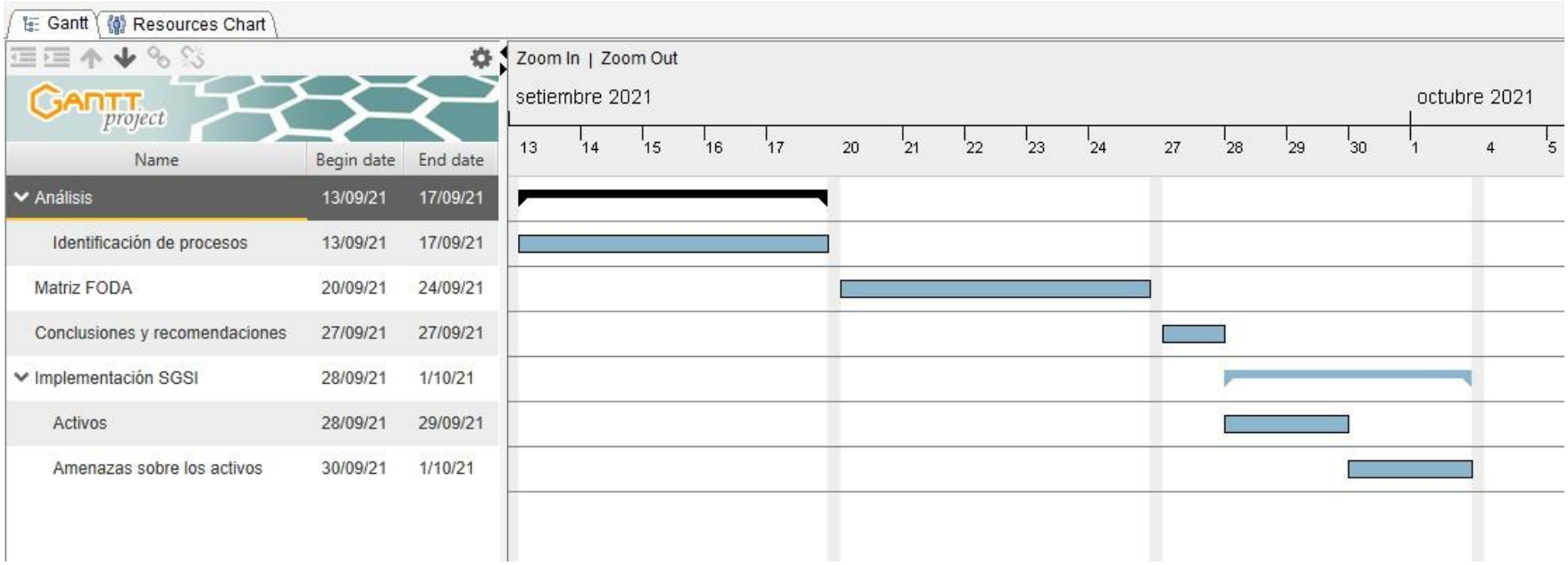
Tabla Nro. 27: Presupuesto

Recurso	**Detalle**	**Cantidad**	**Unidad**	**P. Unitario S/**	**P. Total S/**
Personal	Ingeniero de Sistemas	1	Unidad	2500	2500
	Técnico eléctrico	1	Unidad	270	270
	Costo total de personal				**2770**
Materiales	Alicate de corte	1	Unidad	59	59
	Cutter	1	Unidad	6	6
	Soplete	1	Unidad	69	69
	Destornillador plano - estrella	2	Unidad	12	24
	Alicate de pinza	1	Unidad	30	30
	Brocha para Limpiadora	3	Unidad	15	45
	Costo total de Materiales				**233**
Costo total					**3003**

Fuente: elaboración propia

5.3.4 Diagrama de Gantt

Gráfico Nro. 4: Diagrama de Gantt



Fuente: Elaboración propia

VI. CONCLUSIONES

Se implemento un plan de seguridad informático en el Juzgado de Paz de única nominación del distrito de Canchaque, el cual mejoró el control de datos e información ya que la normativa ISO 27001 nos dice que la seguridad de la información se debe regular en organizaciones ya sean privadas o públicas como es el caso del Juzgado de paz de única nominación Canchaque.

1. Se evaluó la situación actual de la seguridad informática en el Juzgado de Paz de Única nominación del distrito de Canchaque, por lo que se identificó los activos y amenazas, los cuales se encuentran en mi propuesta de mejora y fueron claves para no tener ninguna dificultad o duda al momento de ser realizado dicho plan, esto le favorece al Juzgado ya que no contaba con este registro que es esencial en todo despacho avalado por el estado permitiendo tener los activos junto en un listado y como valor agregado se obtiene el cumplimiento coherente con la evaluación de la situación actual.

2. Se determino el nivel de conocimiento acerca de la seguridad informática actual del juzgado de paz de única nominación, lo cual concluí que 65.00% padece de desconocimiento acerca de las herramientas de la tecnología de la información mientras que el 35.00% si tenía ideas sobre el tema, además esta información concluida me sirvió para ser utilizada en la propuesta de mejora en el aspecto de capacitaciones o charlas informativas que se aplican, pues así el juzgado y la población cuentan con mayor conocimiento acerca de su seguridad informática lo que es un beneficio para que estos temas sobre la seguridad informática sean cada vez más abarcados, por consiguiente se obtiene un valor agregado que mediante las encuestas realizadas se logró ver el nivel de conocimiento para dar una solución factible al problema.

3. Se implemento el plan de seguridad informática en el juzgado de paz de única nominación Canchaque, en el cual termine de completar este plan de seguridad informática con el 100% de ejecución, por lo que, si fue necesario

implementar el plan, además el juzgado ya no está expuesto a tener posibles alteraciones a la información y consecuencias grabes en la perdida de datos de la población u inseguridad al momento de descargar o enviar documentos, esto permite un valor agregado para tener en cuenta con las soluciones más viables de los activos.

VII. RECOMENDACIONES

1. Es conveniente que el Juez de Paz evalúe solicitar a la municipalidad un profesional de servicio técnico o soporte que lo apoye a respecto a si algún activo de su despacho está en una amenaza vidente, el profesional de apoyo será pagado por parte de la municipalidad y además se encargara de tener sus activos en estado normal y funcionales.
2. Es importante tener de consideración que el Juez de Paz utilice programas o software con licencia en sus equipos ya que por su despacho se realizan documentos de suma importancia y de gran relevancia, al utilizar licencia apoya a la No Piratería Informática, su Juzgado se vería seguro y más actualizado el cual lo colocara por encima de otros Juzgados vecinos siendo el primero en usar estas recomendaciones.
3. Para mayor desempeño en el Juzgados es importante considerar que el Juez contrate un especialista en sistemas que creara una tarea especifica de limpieza de acuerdo a los datos obsoletos que se alojan y se guardan en carpetas no utilizables en su PC y esto volverá más rápida las operaciones que le ordenemos al ordenador para así ahorrar tiempo en cada creación o modificación de cualquier documento realizado en su dicho ordenador.
4. Asimismo, le hago presente al Juez que sería relevante gestionar charlas u capacitaciones por parte de la Municipalidad Distrital Canchaque sobre el uso sobre productos de paquetes de oficina, para tener mayor conocimiento y uso del programa de documentación ya que esto le brindará mayor eficiencia, esto le dará mayor conocimiento de sus herramientas que permiten ahorrar tiempo y ganar conocimiento para solucionar futuros errores.
5. Por último, se propone al Juez evaluar el alojamiento de información en la nube, por temas de seguridad ya que el ambiente en el que se encuentra su despacho está expuesto a varias amenazas de sus activos, entre ellos los desastres naturales como movimientos sísmicos los cuales no avisan en qué momento llegan, mientras sus documentos estén en la Nube podrá visualizarlos desde cualquier ordenador o dispositivo móvil con acceso a internet.

REFERENCIAS BIBLIOGRÁFICAS

1. Costas J. Seguridad informática [En Línea]. Madrid: RA-MA Editorial, 2015 [consultado 23 Apr 2021]. Disponible en: https://elibro.net/es/ereader/uladech/62452?page=16

2. Torres C.D., "Plan de seguridad informática basado en la norma iso 27001, para proteger la información y activos de la empresa privada megaprofer s.a." univ técnica ambato fac. 2020;5(1):55. Disponible en: https://repositorio.uta.edu.ec/bitstream/123456789/30690/3/Tesis_t1657si.pdf

3. Chicaiza D., Vinicio C., Plan de seguridad informática basado en la norma iso 27001, para proteger la información y activos de la empresa privada Megaprofer S.A., Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Sistemas Computacionales e Informáticos, Ambato - Ecuador, 2020. Disponible en: https://repositorio.uta.edu.ec/bitstream/123456789/30690/3/Tesis_t1657si.pdf

4. Mollocondo S.M. Análisis de riesgo y políticas de seguridad de información de la oficina de tecnologías de información (oti) – una puno 2018. Univ nac del altiplano esc posgrado [internet]. 2018;105. Disponible en: http://repositorio.unap.edu.pe/bitstream/handle/unap/12303/yana_aydee_quispe_patricia.pdf?sequence=1&isallowed=y

5. Aguirre J. Sistema web para la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en la empresa de Servicios Informáticos S.A.C – La Molina. Esc Acad Prof Ing Sist. 2018;119. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/35308

6. Celis L., Plan de seguridad de la información aplicado a la central hidroeléctrica carhuaquero. Universidad Católica st Toribio Mogrovejo fac ing. 2012;1-53. Disponible en: http://tesis.usat.edu.pe/xmlui/handle/20.500.12423/1615?show=full

7. Solano R.C., Implementacion de un sistema informático de hospitalizacion del hospital elpidio berovides pérez –otuzco; 2018. Univ católica los ángeles chimbote fac ing esc prof ing sist. 2018;151(2):10-7. Disponible en: http://repositorio.uladech.edu.pe/handle/20.500.13032/3033

8. Gálvez G. Implementación de un sistema informático de registro de historias clínicas para el centro de salud de ricardo palma - huarochirí; 2018. Univ católica los ángeles chimbote fac. 2018;151(2):10-7. Disponible en: http://repositorio.uladech.edu.pe/handle/20.500.13032/3043?show=full

9. Merino C. «Implementación De Un Plan De Seguridad Informática Con La Norma Iso/Iec 27001 En La Empresa Ransa Comercial S.A - Piura; 2021.». Universidad Católica Los Ángeles Chimbote / ULADECH [Internet]. https://repositorio.uladech.edu.pe/bitstream/handle/20.500.13032/24698/SEGURIDAD_INFORMATICA_MERINO_ROSAS_CESAR.pdf?sequence=1&isAllowed=y

10. Romero A., Seguridad Informática Y Alta Disponibilidad, Españaies Tiempos Modernos Zaragoza – ESPAÑA. Disponible en: https://migasfree.educa.aragon.es/presentaciones/curso-administracion_linux-gerencia_dga-materiales/PDFs-Documentacion/libro_seguridad_informatica.v14.5.baja_resol.pdf

11. Romero M. I., Figueroa G.L., Vera S., Álava J.E., Parrales G.R., Álava Mero C.J., et al. Introducción a la seguridad informática y el análisis de vulnerabilidades. Introducción a la seguridad informática y el análisis de vulnerabilidades. 2018.

12. Ayala E. y Gonzales S. Tecnologías de la información y la comunicación. Cuad 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

13. Andrada A. Nuevas Tecnologías de la Información y la Comunicación/NTICX. Buenos Aires: Maipue [Internet]. 2010; Disponible

en: http://www.maipue.com.ar/indice/texto/Nuevas tecnologias de la informacion y la comunicacion - NTICX.pdf

14. Hernández A. Los sistemas de información: evolución y desarrollo. Proy Soc Rev Relac laborales. 2003;(10):149-65.

15 López G.M. Grabación de datos [En Línea]. Paracuellos de Jarama, Madrid: RA-MA Editorial, 2015 [consultado 18 Apr 2021]. Disponible en: https://elibro.net/es/ereader/uladech/106472?page=14

16 Mejía J. La investigaión cuantitativa en la sociología peruana Santiago de Chile.CL: Red cinta de Moebio; 2019.

17 Sáez L.J. 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.

18 Hernández R.; Fernández C. Baptista MP. Metodología De La Investigación. V. Chacón JM, editor. México: McGraw-Hill; 2010.

19 Pazmiño C. I. Tiempo de investigar, investigación científica 2: cómo hacer una tesis de grado Quito,Ecuador: EDITEKA Ediciones; 2008.

20 Huincho W., Nuñez Á., Sistema de gestión de seguridad de la información para mejorar la protección informática de la Comisaria Región., Escuela De Formación Profesional De Ingeniería De Sistemas Y Computación, Cerro de Pasco – Perú – 2019.

21 Pérez R.J. Mantenimiento del software (UF1894) [En Línea]. Malaga: IC Editorial, 2016 [consultado 17 May 2021]. Disponible en: https://elibro.net/es/ereader/uladech/44523?page=16

22 Gutiérrez O.E. Comunicaciones móviles y redes inalámbricas [En Línea]. Córdoba: Jorge Sarmiento Editor - Universitas, 2020 [consultado 17 May

2021]._Disponible_en:_https://elibro.net/es/ereader/uladech/172318?page=24

23 Fresno C. ¿Cómo funciona Internet? [En Línea]. Córdoba: Editorial Ciudad Educativa, 2018 [consultado 17 May 2021]. Disponible en: https://elibro.net/es/ereader/uladech/36728?page=55

24 Cernuda del Río A., Gayo A. D., Cueva L. J.M, Benjamín López P. B., Díaz F. M. Á., Tajes M. L., García F. A., Carús V. C., Néstor Cueva L. N., Puerto P. R. M., Pérez D. J. A, Gutiérrez D. Á., Luengo D. C., García F. N., González R. M., Pérez P. J. R., Riesco A. M., Labra G. J. E., Martínez P. A. B., Suárez T. M., García B. C. P., Vinuesa M. L., Fernández L. D., Fernández A. C., Aquilino A, J. F., INFORMÁTICA GENERAL. 1ra ed. España: SERVITEC; 2006. Disponible en: http://di002.edv.uniovi.es/~cueva/publicaciones/monografias/48_InformaticaGeneral.pdf

25 Costas S. J. Seguridad informática [En Línea]. Madrid: RA-MA Editorial, 2015 [25 Sep 2021]. Disponible en: https://elibro.net/es/ereader/uladech/62452?page=16

26 Raya C. J.L. Implantación de sistemas operativos [En Línea]. Madrid: RA-MA Editorial, 2015 [consultado 25 Sep 2021]. Disponible en: https://elibro.ne+t/es/ereader/uladech/62453?page=25

27 La Red M. D. L., Seguridad en los Sistemas Operativos. Corrientes – Argentina; 2007.

28 MAGERIT versión 3 (versión española): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.Edita: © Ministerio de Hacienda y Administraciones Públicas, octubre 2012. - NIPO: 630-12-171-8

29 Rojas E. Tipo de Investigación: Cuantitativa. , Parte en metodología; 2018.

30 Arroyo Guardeño, D. Gayoso Martínez, V. y Hernández Encinas, L. (2020). Ciberseguridad. Madrid, Editorial CSIC Consejo Superior de Investigaciones Científicas. Recuperado de: https://elibro.net/es/ereader/uladech/172144?page=15.

31 Juzgado de Paz de única nominación Canchaque - Piura.

32 Perez L. Perez R. y Seca M.V. Metodología de la investigación científica [En_Línea]. Editorial Maipue, 2020 [consultado 26 Ene 2023]. Disponible en:_https://elibro.net/es/lc/uladech/titulos/138497

33 Chimbote UCLÁd. Comité Institucional de Ética en Investigación. Código de Ética para a Investigación. Documento Institucional de Investigación Chimbote: Rectorado; 2021.

34 Código de ética para la investigación [Internet]. Uladech.edu.pe. 2020 [cited 26 junio 2020]. Disponible en: https://www.uladech.edu.pe/images/stories/universidad/documentos/2019/codigo-de-etica-para-la-investigacion-v002.

ANEXO

Anexo 1: Cronograma de actividades

Gráfico Nro. 5: Cronograma de actividades

CRONOGRAMA DE ACTIVIDADES

N°	Actividades	Año 2020								Año 2021							
		Semestre I				Semestre II				Semestre I				Semestre II			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
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				x												
5	Mejora del marco teórico y metodológico					x											
6	Elaboración y validación del instrumento de recolección de Información						x										
7	Elaboración del consentimiento informado							x									

8	Recolección de datos								x								
9	Presentación de resultados								x								
10	Análisis e Interpretación de los resultados									x							
11	Redacción del informe preliminar										x						
12	Revisión del informe final de la tesis por el Jurado de Investigación												x				
13	Aprobación del informe final de la tesis por el Jurado de Investigación													x			
14	Presentación de ponencia en jornadas de investigación															x	
15	Redacción del artículo científico																x

Fuente: Reglamento de investigación V17(34).

Anexo 2: Presupuesto

DESCRIPCIÓN	CANTIDAD	COSTO UNITARIO	TOTAL PARCIAL	TOTAL
1. RENUMERACIONES				
1.1. Asesor	01	1400.00	1400.00	
1.2. Estadístico	01	200.00	200.00	
			1,600.00	1,600.00
2. BIENES DE INVERSION				
2.1. Impresora	01	250.00	250.00	
			250.00	250.00
3. BIENES DE CONSUMO				
3.1. Papel bond A-4 80	01 m	25.00	25.00	
3.2. Tóner para impresora	01	45.00	45.00	
3.3. CD	02	2.00	2.00	
3.4. Lapiceros	02	1.00	1.00	
3.5. Lápices	02	2.00	2.00	
			75.00	75.00
4. SERVICIOS				
4.1. Fotocopias	50 hoja	25.00	25.00	
4.2. Anillados	3	15.00	15.00	
4.2. Servicios de Internet	70hrs	80.00	80.00	
4.3. Pasajes locales		235.00	235.00	
			355.00	355.00
	TOTAL			2,280.00

Anexo 3: Instrumento de recolección de datos

CUESTIONARIO

TITULO:

IMPLEMENTACIÓN DE UN PLAN DE SEGURIDAD INFORMÁTICO EN EL JUZGADO DE PAZ DE ÚNICA NOMINACIÓN DEL DISTRITO DE CANCHAQUE – PIURA, 2021.

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?	X	

CUESTIONARIO:

Nivel de satisfacción de la implementación de un plan de seguridad informático.	SI	NO
¿Cree usted que si implantamos un plan de seguridad informático ahorraría tiempo en ejecutar cada proceso?		
¿Cree que el plan de seguridad informático ayude a mejorar la administración de los documentos?		
¿Cree Usted que capacitaciones sobre seguridad informática serian de relevante importancia para los trabajadores de este juzgado?		
¿Cree Usted que sería necesario incorporar al juzgado controles de seguridad para el uso de los dispositivos de PC?		

¿En el Juzgado ha ocurrido algún hecho referente a la seguridad informática?		
¿Cree que es necesario aplicar un plan de seguridad informático en el Juzgado?		
Nivel de conocimiento con respecto al uso de las herramientas TIC.	SI	NO
¿Usted sabe la importancia del mal manejo de la información?		
¿Usted considera que con un plan de seguridad informática estará más a gusto (seguro) con su trabajo?		
¿Usted considera que el manejo o tratado de archivos es fácil de realizar		
¿Usted conoce sobre las herramientas Tecnologías de la información y la comunicación (TIC)?		
¿En el Juzgado de Paz realizan capacitaciones sobre seguridad informática?		

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 "Implementación de un plan de seguridad informático en el juzgado de paz de única nominación del distrito de Canchaque – Piura, 2021" y es dirigido por Cutin Zapata Alipio, investigador de la Universidad Católica Los Ángeles de Chimbote.

El propósito de la investigación es: Implementar de un Plan de seguridad informático en el juzgado de paz de única nominación de Canchaque – Piura, 2021, para mejorar la calidad de atención al cliente.

Para ello, se le invita a participar en una encuesta que le tomará 5-10 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.

Si desea, también podrá escribir al correo 0809181121@uladech.pe 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:

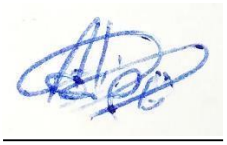
Nombre: _____

Fecha: _____

Correo electrónico: _____

Firma del participante: _____

Firma del investigador (o encargado de recoger información):



Cutin Zapata Alipio
DNI: 71533432

Anexo 5: Autorización de la empresa

"Año del Bicentenario del Perú: 200 años de Independencia""

JUZGADO DE PAZ UNICA NOMINACION CANCHAQUE

10-09-2021 Horas 10:00 AM

SOLICITO: APLICAR ENCUESTAS
POR TEMA DE ESTUDIO
UNIVERSITARIO

SEÑOR JUEZ DE PAZ DE UNICA NOMINCAION

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 8vo ciclo de la carrera Ing. De sistemas, aplicar 10 encuetas por trabajadores de este Juzgado, para un trabajo de temas de estudio, el cual será reflejado en mi tesis, las respuestas solo se utilizarán 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, 10 de setiembre de 2021.

Atentamente.

CUTIN ZAPATA ALIPIO

DNI N° 71533432
CELULAR N° # 928280755

Informe de tesis

INFORME DE ORIGINALIDAD

10%	10%	0%	0%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.uta.edu.ec Fuente de Internet	10%

Excluir citas	Activo	Excluir coincidencias	< 4%
Excluir bibliografía	Activo		