UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

PROPUESTA DE IMPLEMENTACIÓN DE SEGURIDAD INFORMÁTICA EN LAS TIC DE LA I.E. SAN MIGUEL ARCÁNGEL, CATACAOS - PIURA; 2016.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR:

BACH. ANCAJIMA MENDOZA MARÍA ALEJANDRA

ASESOR:

ING. MORE REAÑO RICARDO EDWIN

PIURA –PERÚ

2019

JURADO EVALUADOR DE TESIS Y ASESOR

MGTR. JOSÉ ALBERTO CASTRO CURAY

Presidente

MGTR. JENNIFER DENISSE SULLÓN CHINGA

Secretaria

MGTR. MARLENY SERNAQUÉ BARRANTES

Miembro

ING. RICARDO EDWIN MORE REAÑO

Asesor

DEDICATORIA

Le dedico esta tesis a mis padres Oscar P. Ancajima Sernaqué y Mirian Mendoza Rivas que me brindaron su apoyo incondicionalmente, sus consejos, su paciencia y con infinito amor me han ayudado a atravesar momentos difíciles en lo largo de mi vida. Les dedico esta tesis porque me han dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi esfuerzo, mi optimismo, en que sea siempre perseverante y con ellos el coraje de salir adelante siempre con humildad para así poder conseguir mis objetivos.

A mi familia que gracias a ellos soy lo que soy, a mis hermanos que a pesar de todo han estado conmigo alentándome a no rendirme y porque han fomentado en mí el deseo de superación y de triunfo en la vida, porque sé que ellos siguen mis pasos y quiero darles el mejor ejemplo a seguir.

María Alejandra Ancajima Mendoza

AGRADECIMIENTO

A Dios, por darme la dicha de vivir y por acompañarme en cada paso que doy, por darme la fuerza necesaria para superar los obstáculos y dificultades que se presentaron a lo largo de toda mi vida y por haber puesto en mi camino a personas que han sido mi soporte y compañía durante todo el periodo de estudio.

Papás les vuelvo a agradecer todo lo que han hecho por mí, sobre todo por su paciencia, quiero que sepan que gracias a ustedes soy fuerte y que sin ustedes no soy nada. Por estar conmigo en cada momento y circunstancias que pasaron durante toda mi vida, por hacerme una mejor persona cada día y que gracias a ustedes no hubiera logrado que esta meta se cumpliera.

A las autoridades Universitarias por abrirme las puertas a un mundo nuevo donde me permitieron convertirme ser una gran profesional, a cada maestro que fue parte de este proceso de formación, así mismo agradezco a mis asesores, Ing. Víctor Ángel Ancajima Miñán y el Ing. Ricardo Edwin More Reaño, por apoyarme al momento de realizar esta tesis bajo su dirección guiando mis ideas para poder lograr un buen resultado.

Como también agradezco a mis compañeros, por su apoyo incondicional y la paciencia que me tuvieron en el transcurso de la carrera, a Robert K. Cisneros Ampuero por alentarme tanto a no rendirme, por ayudarme de manera emocional y económica, por estar en cada momento especial de mi vida, por demostrarme que la vida nunca es fácil pero uno puedo salir adelante con la fuerza y las ganas de triunfar, un gran ejemplo a seguir.

Agradezco a la I.E. San Miguel Arcángel de Catacaos, a los docentes que me apoyaron al momento de brindarme su tiempo para poder recolectar datos para el desarrollo de mi investigación y sobre todo a la Dir. ª. Flor de María Rojas Neyra.

María Alejandra Ancajima Mendoza

RESUMEN

La presente tesis se desarrolló bajo la línea de investigación en tecnologías de información y comunicación (TIC) para la mejora continua de la calidad de las organizaciones del Perú de la escuela profesional de Ingeniería de sistemas, la cual estuvo basada en realizar una PROPUESTA DE IMPLEMENTACIÓN DE SEGURIDAD INFORMÁTICA EN LAS TIC DE LA I.E. SAN MIGUEL ARCÁNGEL, CATACAOS - PIURA; 2016. El tipo de la investigación fue cuantitativa, nivel descriptivo, diseño no experimental y de corte transversal; teniendo como objetivo general realizar un estudio de los riesgos que se tiene en la institución, y así brindar una buena propuesta de implementación de Seguridad Informática de la I.E. San Miguel Arcángel, la cual mejorará el control de seguridad de la institución y se tendrá un mejor manejo en las herramientas tecnológicas por los docentes, personal administrativos y alumnos. Con una población muestral de 60 personas entre docentes, alumnos y personal administrativo que utilizan los equipos tecnológicos dentro de las áreas dentro de la institución. Se obtuvieron como resultados el 75.00% de los encuestado expresó que se encuentran satisfechos con las TIC en el proceso de enseñanza, así mismo el 73.00% expresó que se encuentran satisfechos con la formación y capacitación sobre el manejo de las TIC y el 73.00% de los encuestado expresó que se encuentran satisfechos con la seguridad Informática en las TIC en la institución. Por lo que se puede concluir que las políticas ayudarán en la Seguridad Informática de la institución permitiendo que los docentes, alumnos y personal administrativo queden satisfechos en el momento de utilizarlas, sintiéndose seguros a través de ellas y esta pueda ser más fácil manejar.

Palabras claves: Control, Seguridad Informática, TIC.

ABSTRACT

This thesis was developed under the line of research in information and communication technologies (ICT) for the continuous improvement of the quality of organizations in Peru of the professional school of Systems Engineering, which was based on making an IMPLEMENTATION PROPOSAL OF IT SECURITY IN IT ICT SAN MIGUEL ARCÁNGEL, CATACAOS - PIURA; 2016. The type of research was quantitative, descriptive level, non-experimental and cross-sectional design; having as general objective to carry out a study of the risks that one has in the institution, and thus to offer a good proposal of implementation of Information Security of the I.E. San Miguel Arcángel, which will improve the security control of the institution and will have a better use of technological tools by teachers, administrative staff and students. With a sample population of 60 people among teachers, students and administrative staff that use technological equipment within the areas within the institution. 75.00% of the respondents expressed that they are satisfied with ICT in the teaching process, likewise 73.00% expressed that they are satisfied with the training and training on the management of ICT and 73.00% of The respondents expressed that they are satisfied with IT security in ICT in the institution. So we can conclude that the policies will help in the Information Security of the institution allowing teachers, students and administrative staff to be satisfied at the time of using them, feeling safe through them and this can be easier to manage.

Keywords: Control, IT Security, ICT.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

I. INTRODUCCIÓN

Gómez (1), indicó que es importante contar con políticas de seguridad bien concebidas y efectivas, que pueda proteger la inversión y los recursos de información de una empresa. Al implementarse una política de seguridad esta mantendrá más protegida la información que se encuentra en la red, evitando los accesos indebidos de personas externas.

Actualmente los cambios que surgen en el mundo moderno, incorpora en alto el volumen de información y los múltiples sistemas que la proveen generan el aumento de las vulnerabilidades y las amplias amenazas cibernéticas, por lo que la seguridad va más allá de mecanismos de protección y sin políticas de seguridad correctamente implantadas nuestra información puede ser plagiada y compartida, afectando en el buen desempeño, prestigio y el correcto funcionamiento de la institución (2)

Dado que hoy en día la mayoría de las instituciones educativas tienen información valiosa la cual se requiere que tenga la seguridad necesaria para que no pueda ser extraída por individuos; en la I.E San Miguel Arcángel ubicada en el distrito de Catacaos, cuenta con buenas TIC las cuales no son utilizadas correctamente; por lo que la información corre mucho riesgos tanto de ser eliminada o plagiada, por lo que esto se ha vuelto un problema dentro de la institución.

Lo que se espera en este proyecto es que la Institución Educativa San Miguel Arcángel tenga un buen manejo de las TIC para la Seguridad de su información y que los docentes tengan más confianza al momento de guardar la información académica, dado que se pueda implementar una buena política de seguridad para estas. En esta tesis se plantea la propuesta de implementación de Seguridad Informática en las TIC para que la institución educativa San Miguel Arcángel pueda tener un buen manejo en estas herramientas de trabajo.

Debido a las inconsistencias encontradas en la organización se planteó la siguiente pregunta: ¿Es necesaria la propuesta de implementación de seguridad informática en las TIC de la I.E San Miguel Arcángel, Catacaos - Piura; 2016?

Se tuvo como objetivo general, realizar la propuesta de implementación de Seguridad informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016, para mejorar el control de riesgos informáticos.

Se dieron los siguientes objetivos específicos:

1. Identificar el estudio de la Seguridad Informática existente dentro de la I.E San Miguel Arcángel.

2. Evaluar los diferentes efectos del manejo de las herramientas TIC en la I.E. San Miguel Arcángel.

3. Comparar los diferentes dominios o áreas que se deberán tomar en cuenta según las mejores prácticas con el fin de formular estrategias para la seguridad Informática en la I.E. San Miguel Arcángel.

4. Desarrollar una buena metodología basada en las mejores prácticas para que cualquier organización pueda desarrollarlo teniendo una seguridad Informática de alta calidad con las políticas establecidas.

La justificación dentro de la investigación se basa en que actualmente se encuentra en la necesidad de proteger las fuentes de información, incluyendo instalaciones físicas, base de datos y redes, han producido una demanda de estrategias y TIC. Por lo general el rol de la tecnología, ha tomado fuerza en la vida no solo de alumnos o jóvenes, sino que también abarca a los adultos, haciendo que los docentes puedan capacitarse en el manejo de las TIC para un buen desarrollo de información para el dictado de sus clases.

Estos últimos años se han desarrollado diferentes tecnologías que brindan una oferta muy grande de recursos de entretenimiento así como de educación, y el manejo de la seguridad informática. Está gran diversidad de recursos permite mantener la privacidad de la información desarrollada por el mismo docente, alumno y de la misma institución evitando que cualquiera tenga acceso.

Al investigar este tema, la seguridad informática involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deberán tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran. Cabe mencionar que la seguridad es un proceso continuo de mejora por lo que las políticas y controles establecidos para la protección de la información deberán revisarse y adecuarse, de ser necesario, ante los nuevos riesgos que surjan, a fin de tomar las acciones que permitan reducirlos y en el mejor de los casos eliminarlos (3).

Toda la información es recopilada, almacenada y es puesta a la disposición de los usuarios en este caso de los docentes y/o personal administrativo, a través de las computadoras y transferida a través de las redes entre los ordenadores. En caso de que la información de la Institución Educativa caiga en manos incorrectas; volviéndose vulnerable a la pérdida de credibilidad no solo por parte de todos los docentes sino también por parte de los padres de familia y/o alumnos llevando al quiebre institucional. Por lo cual, se deberán buscar las mejores políticas de seguridad para proteger la información de la Institución, es un requisito importante que debe tener cualquier organización, y en muchos casos también un imperativo ético y una obligación legal.

Existen diferentes estudios y análisis que muestran una tendencia creciente en cuanto a incidentes de seguridad en el ciberespacio. Por ejemplo, el CERT (Computer Emergency Responce Team) (4), dio a conocer un incremento

significativo en el número de incidentes de seguridad que le fueron reportados durante los años 2000 y 2001. Las repetitivas amenazas al robo de información en general se presentan tanto de fuentes internas como externas en las organizaciones. Estas amenazas van desde extracción de datos de forma ilegal (fuga de información) hasta la destrucción o alteración maliciosa de datos valiosos, por lo que es de vital importancia identificar estas amenazas para determinar la vulnerabilidad de las Tecnologías de Información y crear estrategias claves para establecer una buena Seguridad Informática a la Institución. Esto nos sirve como referente para darnos cuenta de los riesgos genéricos que tiene la Seguridad Informática y si es que las Tecnologías de Información son utilizadas correctamente, estos recursos son ejecutados tanto en lo académico como en la seguridad del ingreso de los docentes. En contraste podríamos conocer las tendencias de uso de los alumnos y docentes para generar recomendaciones, si solo lo está usando para el ocio o el entretenimiento.

La investigación se justifica operativamente, en mejorar la seguridad de información de los docentes, alumnos y personal administrativo, brindándoles políticas de seguridad e información del manejo adecuado de las TIC dentro de la institución.

La implementación de la Seguridad Informática en las TIC ayudará a que los docentes, alumnos y personal administrativo tengan un mejor manejo de su información, además podrán hacer sus actividades con más confianza, por lo que se justifica económicamente, en que la institución se ve favorecida en la reducción de costos, ya que al implementarse estas políticas de seguridad no generan costos excesivos, permitiendo el ahorro a la institución.

Se justifica tecnológicamente en que la institución cuenta con los equipos tecnológicos adecuados para que toda la información sea recopilada, almacenada y es puesta a la disposición de los usuarios en este caso de los docentes y/o personal administrativo, a través de las computadoras y transferida a través de las redes entre los ordenadores.

Por ello nos abocamos en la I.E. San Miguel Arcángel para determinar en qué medida ayudan las políticas en la Seguridad Informática dentro la institución. Los docentes, alumnos y personal administrativo son los principales protagonistas dentro de la institución, por lo que se debe tener cuidado ya que es más probable que se sufra un plagio y/o robo de la información.

Por lo cual las políticas permitirán lo siguiente:

- Facilitar un determinado acceso de la información de la institución.
- Facilitar a los docentes buscar la información de sus alumnos y/o material brindado por el estado.
- Facilitar el acceso completo de toda la información en el caso de la directora de la institución.
- Facilitar que la información sea guardada y manejada de manera segura.

La presente investigación se llevó a cabo en el área de informática en la I.E. San Miguel Arcángel, distrito de Catacaos, provincia de Piura, por lo que la Seguridad informática debe tener un mayor alcance, ya que para los docentes, alumnos y personal administrativos es importante que la información de la institución este segura ante robos y/o plagios. Se utilizó el tipo de investigación cuantitativa, nivel descriptivo, diseño no experimental de corte transversal.

II. REVISIÓN DE LITERATURA

2.1. Antecedentes

2.1.1. Antecedentes a Nivel Internacional

Ramas (5), en su libro "TIC en educación: escenarios y experiencias", publicado en el año 2015, en la ciudad de México, el cual nos habla sobre cómo han afectado las TIC en el mundo de la educación, especialmente el internet, abordando las dimensiones y criterios fundamentales teniendo un crecimiento exponencial a nivel mundial, llevando a la tecnología a ocupar muchos puestos modificando canales de comunicación. Las instituciones educativas de todos los niveles escolares no pueden moverse sin las TIC, las cuales han abordado las diferentes prácticas pedagógicas, para el uso y apropiación de la misma, tanto en docentes como alumnos. Se trata de identificar las necesidades de los docentes y el nivel del uso de las TIC para así poderles mostrar el manejo y uso adecuado de estas, para que puedan ser implementadas en su actividades de aprendizaje a partir del diseño, desarrollo y aplicación de situaciones de enseñanza, por lo que se realizó un estudio para conocer cuántos alumnos conocían el uso de las TIC, el cual se obtuvo un resultado del 70.00% de alumnos no tienen habilidades para el uso de las TIC en su aprendizaje y desconocen el uso de varias herramientas, más tienen gusto por el entretenimiento, teniendo como conclusión que los docentes para poder utilizar mejor las TIC deben de seguir un módulo dinámico con sus alumnos e interactuar como ellos haciendo un buen uso de los recursos tecnológicos, utilizando un portal web donde los alumnos y docentes puedan subir tareas o enviar información requerida de clase a su E-mail.

La tesis de Bermúdez y Bailón (6), titulada "Análisis en Seguridad Informática y Seguridad de la Información basado en la Norma ISO/IEC 27001- Sistemas de Gestión de Seguridad de la Información dirigido a una Empresa de Servicios Financieros", desarrollada en Guayaquil en el mes de Marzo de 2015, cuyo trabajo tenía como mayor importancia la búsqueda de las vulnerabilidades en la que se encuentra expuesta la información por la falta de controles de seguridad, para así proponer una metodología de implementación teniendo en cuenta la Norma ISO/IEC 27001, estableciendo mecanismos para mitigar los riesgos que presenta el uso de sistemas y manejo de información; teniendo como resultado que el 67.00% de los funcionarios, en general indican que es importante con contar con políticas de Seguridad de la información llegando a la concusión, que el análisis realizado demuestra que la información de las áreas correspondientes y la situación actual en la que nos encontramos refleja potenciales de riesgos, por lo que es conveniente elaborar un manual de políticas de seguridad donde sean detallados controles de seguridad acorde a la realidad y necesidades de la empresa.

Paula y Rosario (7) , en su Tesis "Análisis de la Gestión de la Seguridad de Tecnologías de la Información (TI),en las Pequeñas y Medianas Empresas de San Francisco de Macorís" en República Dominicana en el año 2014, hace un desarrollo complejo en la búsqueda de las Tecnologías de Información mostrando desde que estas se iniciaron hasta en lo que se han convertido hoy en día, mostrando no solo lo bueno de ellas sino también lo que puede pasar si es que no se tiene en cuenta la seguridad que permite asegurar la confidencialidad, la integridad y la disponibilidad de las informaciones, datos y servicios de TI de una organización. Dando a conocer dicha investigación que si bien se da la seguridad en las TI, estas no cumple con normativas dentro de la organización, el

91.00% de las empresas PYME indicaron que si es posible un alto del nivel de riesgo tecnológico al que están expuestas y el 9.00% no tiene ideas del nivel de riesgo tecnológico al que se encuentran expuestas. En tal sentido, sobre si tienen o no estimado, o identificado el posible impacto ante la ocurrencia de un evento de seguridad de la información el 55.00% de las empresas entrevistadas si tienen estimado o identificado el posible impacto ante la ocurrencia de un evento de la seguridad de la información y el 45.00% no tiene nada estimado ni identificado. Llegando a indicar que es bueno brindarles información a toda empresa para que cuenten con un plan de seguridad creando políticas que establecerán bases para una correcta gestión de calidad.

En el libro de Chicano (8), titulado "Gestión de incidentes de Seguridad Informática" desarrollada en el año 2014, detalla detenidamente cada riesgo que corre la información, determinando que las organizaciones deben definir políticas de seguridad más drásticas en las TIC para evitar el mal acceso a personal no autorizado impidiendo el malintencionado uso de los datos ya que los atacantes cada vez van utilizando técnicas más sofisticadas para llevar acabo sus ataques y, por ello, la detección de evidencias y el posterior análisis de las mismas puede ser una tarea bastante tediosa para los investigadores, por lo que en una organización su información más valiosa no se almacena en redes generales, sino que son utilizadas otras subredes que son separadas para aumentar su nivel de seguridad y ser tratadas con un mejor modo de acuerdo al valor de estas. Este libro nos da a conocer los distintos tipos de ataques y como prevenirlos y combatirlos, en particular como saber identificar y caracterizar los diferentes datos del funcionamiento de las TIC, todo ello de la mano de las políticas de Seguridad.

Gómez (1), en su Libro titulado "Auditoría de Seguridad Informática" , fue impreso en el mes de Setiembre de 2014 en

España, con la finalidad de identificar los riesgos, amenazas, etc. que puedan tener las empresas a través de la redes teniendo una planificación detallada de estas, ya que las características que priman en el entorno de cualquier entidad moderna, que incorpore a su gestión las TIC, sustentadas sobre una infraestructura tecnológica con amplio grado de integración de redes, comunicaciones y sistemas de información de punta, para maximizar a través de su soporte logístico el control interno, la contabilidad, y consecuentemente sus resultados, demanda transformaciones en la práctica de la disciplina orientada a ejercer un control superior, lo cual se realiza una serie de encuestas a los usuarios, teniendo como resultados que no solo se viola la seguridad en las TIC sino que también hay violaciones en las políticas de seguridad y no hay confiabilidad en estos, llegando a la conclusión que las organizaciones que operan o centran gran parte de su actividad a través de las TIC necesitan ser dotados de buenas políticas y tener las medidas de protección adecuadas que garanticen el continuo desarrollo y sostenibilidad de sus actividades.

En el libro de Arnedo (9), denominado "Redes de Comunicaciones" publicado en el mes de noviembre de 2013, a necesidad apremiante de tener una transmisión segura de los datos es evidente, cada vez las empresas e instituciones dependen más de los sistemas de redes de datos, se transmite una mayor cantidad de información que necesita estar en la más profunda privacidad, a medida que hace más necesario la capacidad de aprovechar al máximo las tecnologías de red, siguiendo el conjunto de políticas o normas que contribuyen no solamente a la homogenización de la seguridad, sino que además ayuda a los administradores a tener una guía y un marco de referencia al momento de asegurar sus redes y sistemas, así como para poder evaluar la seguridad de una red y poder establecer los mecanismos necesarios para que las empresas alcancen

certificaciones de estándares internacionales de seguridad (como, por ejemplo, ISO 17799 o ISO 27001), lo cual produce sistemas confiables, homogéneos y que por lo tanto serán cada vez más utilizados y ayudarán al hombre a un mejor y más limpio desarrollo.

González (10), en su Tesis Magistral "Estrategias para Optimizar el uso de las TIC y su Seguridad Informática en la Práctica Docente que Mejoren el Proceso de Aprendizaje", realizada en la Institución Educativa Cascajal del Municipio de Timaná- Colombia en el año 2012, realizándose bajo el enfoque cualitativo donde se aplicaron instrumentos como la entrevista y la observación a docentes y alumnos con el objetivo de determinar la manera como se puede optimizar el uso de las TIC, la forma de que estas tengan Seguridad y para que la práctica docente mejore el proceso de aprendizaje, obteniendo como resultados agrupados por categorías construidas a través de un proceso de codificación y comparación constante de los datos recolectados estableciendo relaciones y explicaciones que llevan a responder la pregunta de investigación ¿De qué manera se puede optimizar el uso de las TIC y la Seguridad Informática que esta debería tener en la práctica docente mejore el proceso de aprendizaje en la Institución Educativa Cascajal del municipio de Timaná Departamento del Huila, Colombia?, llegando a la conclusión que los docentes presentan dificultades en el uso técnico y didáctico de las TIC haciendo que la seguridad informática no sea tan factible y ellos siguen realizando prácticas educativas tradicionales.

2.1.2. Antecedentes a Nivel Nacional

En la tesis de Martínez (11), "Implementación de un Sistema de Control de acceso a red en la Empresa Sima" realizada en el año 2018 en Chimbote, este informe muestra la necesidad de

implementar un sistema de control de acceso a la red contando con cuentas de usuarios y la seguridad de ello, ya que en el contexto empresarial siempre es exigido que en la red de datos siempre se lleve un control y sean supervisadas para la protección de la información relevante que puede ser robado o hackeada por cualquier usuario, teniendo como guía la norma técnica Peruana NTP-ISO/IEC 27001:2014, cláusula A.9.4 que establece la política de control de acceso a redes, cuyos diversos controles mencionan utilizar mecanismos de autenticación para controlar el acceso de los usuarios por lo que tiene como resultado que el 50.00% de usuarios no está satisfecho por la atención que se le pone, asimismo el 100.00% de usuarios encuestados indica que es necesario la implementación de un sistema de control de acceso a red, generalizando la mayor conciencia sobre la importancia que tiene la seguridad informática reduciendo los costos por perjuicios en caso de ocurrir siniestros, llegando a la conclusión que esto se puede evitar si toman las medidas de seguridad necesarias con las políticas de seguridad establecidas.

Villanueva (12), en su tesis titulada “Diseño del sistema de gestión de seguridad de la información para el grupo SIAS SAC” desarrollada en la ciudad de Chimbote en el año 2017, el cual se realizó una investigación para poder establecer políticas de seguridad en la organización al igual que la implementación de las TIC. Se contó con una población muestra constituida por 60 trabajadores del Área administrativa de la Oficina Principal, determinándose que: 100.00% de los trabajadores encuestados expresaron que NO existen políticas de seguridad de la información en el GRUPO SIAS SAC. Y que el 78.33% de los trabajadores encuestados NO tienen conocimiento acerca de las políticas de seguridad de la información en las labores administrativas que ellos realizan dentro la empresa. Teniendo como resultados permiten

afirmar que las políticas de seguridad son importantes y resulta beneficiosa el diseño del sistema de gestión de seguridad de la información para el GRUPO SIAS SAC. – Chimbote.

En la tesis de Castillo (13), titulada "Sistema de Gestión de Seguridad de la Información en la Municipalidad Distrital de Pira aplicando la Norma ISO/IEC 27001:2013" en el año 2016 en el departamento de Huaraz, ha realizado una investigación debido a que las medidas de control para satisfacer los requisitos mínimos en seguridad han sido efectivas sólo parcialmente por lo que se diagnosticó la situación actual de la municipalidad, el cual se desarrolló el SGSI basado en la fase de planeación de la norma ISO/IEC 27001:2013 y en los controles, utilizando como metodología de análisis de Gestión del Riesgo MAGERIT versión 3.0. Orientado a todos los sectores de la organización, es decir, administradores de sistemas de gestión de seguridad de la información. MAGERIT se aplica a los sistemas de información de toda la Municipalidad Distrital de Pira, incluyendo los computadores personales y las redes. Indica que el 93.00% de encuestados consideran por conocimiento que en la Municipalidad, este proceso está en el nivel Inexistente, según los niveles de madurez de la ISO/IEC 27001:2013, lo que significa que se reconoce la necesidad de recolectar y evaluar información sobre los procesos de monitoreo, por lo que es factible tener un conjunto de políticas de seguridad informática que garantice la integridad de la información.

En el proyecto de Alcántara (14), denominada "Guía de Implementación de la Seguridad basado en la Norma ISO/IEC 27001, para apoyar la Seguridad en las TIC de la comisaria del norte P.N.P en la ciudad de Chiclayo" desarrollado en el año 2015, para la obtención de dicha información y recolección de datos se consideró conveniente el uso de las técnicas de recolección de datos tales como

encuestas, entrevistas, entre otros para luego extraer la información necesaria y así poder medir la problemática apoyada en el uso de la Norma ISO/IEC 27001, lográndose determinar que el 76.00% de policías involucrados manifestaron que existe un alto grado de inseguridad en el uso de sus aplicaciones. Esta inseguridad está reflejada en varios aspectos como por ejemplo: desactualización de equipos, ausencia de políticas de seguridad, activos vulnerables, etc. Así mismo el 67.00% del total de encuestados indica que la causa presente es que no existe una política adecuada de actualización periódica creando deficiencias para mejorar los niveles de seguridad y confiabilidad en las TIC de dicha institución, hallando como resultado la forma real, que al incorporar la norma ISO/IEC 27001 basada en una Guía de Implementación, teniendo como conclusión que se lograron incrementar los procedimientos utilizados en favor de la Institución permitiéndole la detección de anomalías en la seguridad informática, reflejado en distintos mecanismos de seguridad para salvaguardarla a través de conexiones de Red con el Plan de tratamiento de Riesgos, se permite la disminución de los niveles de riesgos con respecto a los activos de información, considerados amenazas y vulnerabilidades en la institución, esto manifestado en un plan adecuado para abordarlos y tomar las precauciones necesarias que minimicen sus impactos, por lo que yo considero que esta información servirá demasiado en mi trabajo de investigación.

En la Tesis de Gil (15), titulada "Implementación de mecanismos de Seguridad Informática para el mejoramiento, integridad y protección del software del ITP CITEC del norte", en la ciudad de Chimbote en el año 2015, nos indica que se encontró que el 90.30% de los trabajadores indica que no había ningún tipo de seguridad informática, visualizando diferentes problemas en los ordenadores. De acuerdo a ello, se implementó el servidor WSUS, el servidor

FTP, el Antivirus ESET Smart Security, el SuperAntiSpyware, además se configuró la red inalámbrica WiFi y la instalación de un Firewall, para disminuir los problemas de seguridad en el sistema operativo del ITP CITEC del Norte, asimismo el 100.00% de los trabajadores indicó que la institución contaba con algún tipo de seguridad informática; y el 93.50% refirió que los problemas de seguridad en los ordenadores han disminuido. Concluyendo que la implementación de mecanismos de seguridad informática, protegen al sistema operativo de posibles ataques y problemas informáticos, generando mayor nivel de seguridad para la protección del software del ITP CITEC del Norte.

2.1.3. Antecedentes a Nivel Regional

Agramonte (16), en su tesis titulada "Auditoría del Sistema de Seguridad de información en el Hospital III José Cayetano Heredia" efectuada en el distrito de Castilla, departamento Piura en el año 2016, su investigación permitió mejorar la gestión de la información, de acuerdo a las características esta investigación se utilizó la técnica de encuesta, donde la población quedo delimitada en 13 trabajadores de la División Soporte Informático del Hospital quienes tienen relación directa con el tema de la investigación. De acuerdo con los resultados obtenidos se observó: que el 38.00% de los trabajadores encuestados expresaron que la actual seguridad lógica se encuentra en un nivel bajo; el 69% de los trabajadores encuestados indicaron para la seguridad de las aplicaciones el nivel no es bueno y finalmente el 55.00% de los trabajadores encuestados refirieron también en el nivel no es bueno para la Actual administración del centro de procesamiento de datos; con lo que concluyo que el nivel de Seguridad del Sistema de Información del Hospital III José Cayetano Heredia; Castilla, se encuentra en el nivel no bueno, según los niveles de madurez del modelo de referencia de COBIT 4.1.

En la tesis denominada “Servidor Señuelo Informático Honeynet Híbrido y su influencia en la Seguridad Informática Activa Lógica del Centro de Diálisis Piura”, realizada en el año 2014, Figueroa (17), su metodología está basada más en el ámbito de Salud, pero también se concentra más en el punto de la Seguridad informática ya que actualmente los datos de los pacientes se encuentran de manera digitalizada, contando con herramientas TIC como es las conexiones de red para poder proteger la privacidad de los datos, teniendo como resultado implementar una herramienta que protege la información de los pacientes de una manera efectiva con un bajo costo de inversión, teniendo en cuenta los ataques en los que este expuesta la información para luego centrarse en las honeynets, explicando arquitecturas y diferentes generaciones, indicando como resultado que a generalización de encuestas el 100.00% solicita la seguridad de información en máxima calidad dentro de la organización, llegando a la conclusión que la implementación de Honeynet está fuertemente asociada a la disminución de las vulnerabilidades de la red.

Bocanegra (18), realizó una tesis titulada “Perfil del nivel de gestión del dominio adquirir e implementar de las Tecnologías de la Información y Comunicación (TIC), en el personal docente del I.S.T Hermanos Cárcamo” en el año 2013, realizada en la ciudad de Paita, Piura; el cual nos habla de las TIC como han ido influenciando en todos los ámbitos, tanto en lo social como lo educativo, desarrollando con ello la toma de decisión por parte de la adquisición a nuevas tecnologías sin saber el manejo de estas. Por lo cual se realiza la investigación para poder identificar las dificultades y urgencias dentro de la institución indicando el 62.00% estimó que no es bueno el nivel de gestión del proceso adquirir y mantener software aplicativo, mientras que el 86.00%, estimó que tampoco en el nivel de gestión del proceso adquirir y mantener infraestructura

tecnológica de las TIC, de igual manera para el proceso de facilitar la operación y uso de las TIC, el 95.00% no tienen muy buen manejo de ellas.

Zapata (19), en su Monografía denominada "Perfil del nivel de gestión del dominio planeamiento y organización de las Tecnologías de Información y Comunicación (TIC) en el personal docente de la Institución Educativa Ignacio Sánchez", realizada en el departamento de Piura, en el año 2013, tiene como metodología un análisis de los posibles riesgos a cuales pueden estar expuestos sus equipos tecnológicos y sistemas de información, realizando el plan de propuesta de mejorar el nivel de gestión del dominio de las TIC en los docentes de la institución, esto indicara las acciones que deberán tomarse inmediatamente tras un desastre que se pueda dar, por lo que es necesario la identificación previa de cuales de los procesos son críticos y cuáles son los recursos necesarios para garantizar el funcionamiento de las aplicaciones de gestión, por lo que tienes como resultado que el plan de Contingencia de proveer mecanismos de recuperación para los registros vitales y para una buena seguridad informática, teniendo como resultados en su investigación que el 60.80% de los docentes mencionaron que es bajo el nivel de gestión del proceso y manejo de las TIC, mientras que el 56.10% indica que el proceso de determinación de procesos no es bueno, así mismo el 73.17% menciono que no es nada bueno el nivel de calidad en el uso de TIC como conclusión que se debe buscar un buen dominio planeamiento, y que este sea adecuado y vaya acorde a la Seguridad informática para que así se pueda evitar cualquier desastre informático.

Ramos (20), en su tesis titulada “Propuesta de un Plan De Auditoria Informática para el "Sistema de Información En Salud" y el "Aplicativo Para El Registro De Formatos SIS" en los establecimientos de Salud de la unidad ejecutora 400”, en la Región Piura en el año 2015, la propuesta del plan de auditoría informática se ha realizado en base a la Guía de Control Interno de las entidades del Estado Peruano para realizar un análisis de riesgos de ambos sistemas de información basadas en encuestas aplicadas a 10 establecimientos de salud, además se aplicó la Norma Técnica Peruana ISO 27001: 2008 con la finalidad de establecer los objetivos y procedimientos de control adaptados a los establecimientos de salud para posteriormente plasmarlo en el programa detallado de auditoría informática y aplicarlo en un futuro mediante el papel de trabajo por cada procedimiento de control.

2.2. Bases Teóricas

Las bases teóricas, permitirán aclarar los conceptos relativos para la propuesta de implementación respecto a la Seguridad Informática en las TIC para una organización.

El objetivo general de la investigación trata sobre: “Proponer la implementación de Seguridad informática en las TIC de la I.E. San Miguel Arcángel, la cual mejorará la seguridad informática de la institución y se tendrá un mejor manejo en las herramientas tecnológicas, por los docentes, alumnos y personal administrativo”.

2.2.1. El rubro de la empresa

La I.E. San Miguel Arcángel es una institución pública dedicada al rubro educativo, brindando una excelente educación a los alumnos

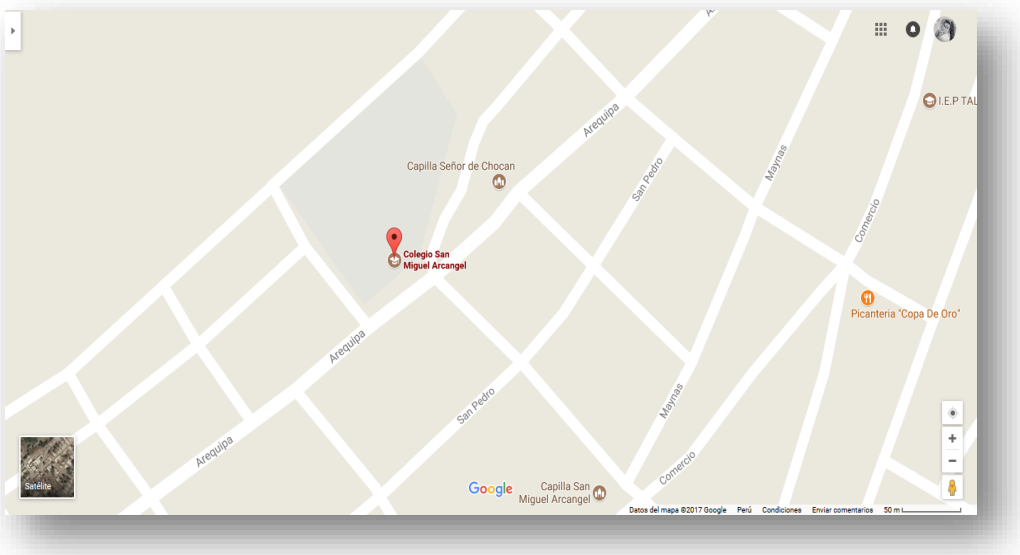
del distrito de Catacaos y sus alrededores, contando con la supervisión constante de los directivos de la DRE (21).

2.2.2. Institución Investigada

Ubicación:

Dirección: Jr. Arequipa S/N – Monte Sullón, Catacaos

Gráfico Nro. 01: Mapa

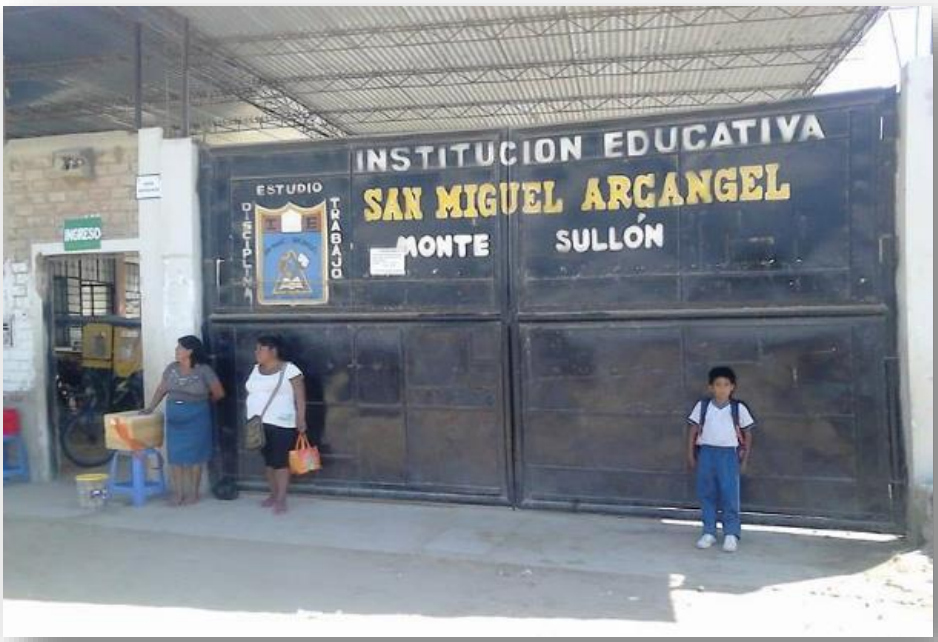


Fuente: Google Maps (22)

Gráfico Nro. 02: Imagen Satelital de la Ubicación

Fuente: Google Maps (22)

Gráfico Nro. 03: Frontis de la Institución Educativa San Miguel Arcángel"



Fuente: Fotografía propia

Historia

En octubre de 1950 con la resolución suprema N° 821, fue creada la Institución Educativa, funcionando a inicios como escuela N° 14036 dirigida por su Directora fundadora Lucila Ceballos y la profesora Delia Saavedra quien con su esfuerzo y dedicación la convirtió en una de las principales Instituciones del distrito de Catacaos. En el año 1996 mediante resolución directoral Regional N° 1455 a la Institución se le asigna el nombre de "San Miguel Arcángel". En el año 2000 fue inscrita ante los registros públicos definitivamente en propiedad del estado. En la actualidad la institución cuenta con una población estudiantil de 1400 alumnos, 18 secciones del nivel primario y 17 secciones en el nivel secundario. Tiene una infraestructura moderna con laboratorios de química, salas tecnológicas y han sido beneficiadas con los programas del Ministerio de Educación, como es: La Jornada Del Escolar completa en el nivel secundario, el Programa de Fortalecimiento del Deporte y el Programa Qaliwarma. Además su plana docentes está conformada por 53 docentes profesionales de alto nivel que han asumido el reto de formar ciudadanos con valores y altamente competitivos, distribuidos en el nivel primario y secundario respectivamente, también cuentan con un sistemas administrativo integrado por 01 secretaria, 01 administrador, 04 coordinadores, 03 auxiliares de soporte pedagógico y 03 personas de mantenimiento; en coordinación de la directora FLOR DE MARÍA ROJAS NEYRA, cuya dirección y capacidad se ve reflejada en la participación de los alumnos en los diversos concursos y presentaciones locales y regionales. La institución tiene 67 años de vida institucional al servicio de la Educación y la cultura del distrito de Catacaos, en esta ALMA MATER, se han formado hombres y mujeres de éxito, profesionales que brillan con luz propia en la sociedad y que buscan el desarrollo, progreso y bienestar de nuestro país (21).

Misión

Son una Institución Educativa de Educación Básica Regular inclusiva del ámbito rural del distrito de Catacaos que proporciona a los niños, púberes y adolescentes una formación integral de calidad en valores, que promueve el logro de sus capacidades, de acuerdo al diseño curricular, emitido por el Ministerio de Educación, donde se atiende las necesidades e intereses de los alumnos, relacionándolo al trabajo pedagógico con el calendario de la comunidad, así mismo cuida el medio ambiente respetando las costumbres de su localidad, provincia y región (21).

Visión

Tiene como visión ser una Institución Educativa Básica Regular inclusiva que brinde hasta el 2021 una educación de calidad con profesores calificados, basada en la práctica de valores que garantice el aprendizaje significativo y la formación, que le brinde de manera permanente el logro de los aprendizajes fundamentales como el apoyo del avance de la Ciencia y Tecnología para un desarrollo Personal y Colectivo, que permita el aprovechamiento adecuado de los recursos, respetando toda forma de vida en la conservación del medio ambiente para satisfacer las necesidades básicas de la comunidad y generar trabajo (21).

Infraestructura Tecnológica

Tabla Nro. 01: Resumen de hardware I.E. San Miguel Arcángel

HARDWARE				
Tipo / Clase	**Descripción**	**Cantidad**	**Capacidad**	
			RAM	**Disco duro**
Estaciones de Trabajo				
PC de escritorio	Lenovo Windows 7	55	4 GB	300 GB
Laptops	Lenovo Windows 7 y 8	105	4 GB	500 GB
Impresoras	Epson l355	02		
Microscopio	ENOSA	01		
Proyector multimedia	Epson s31+	01		
Comunicación				
Switches	Cisco 2960	02		
LAN Cableado Estructurado - Topología estrella, Categoría 5e		100%		
Procesador PC y Laptops		Core i3/ Core i5		

Fuente: Elaboración Propia.

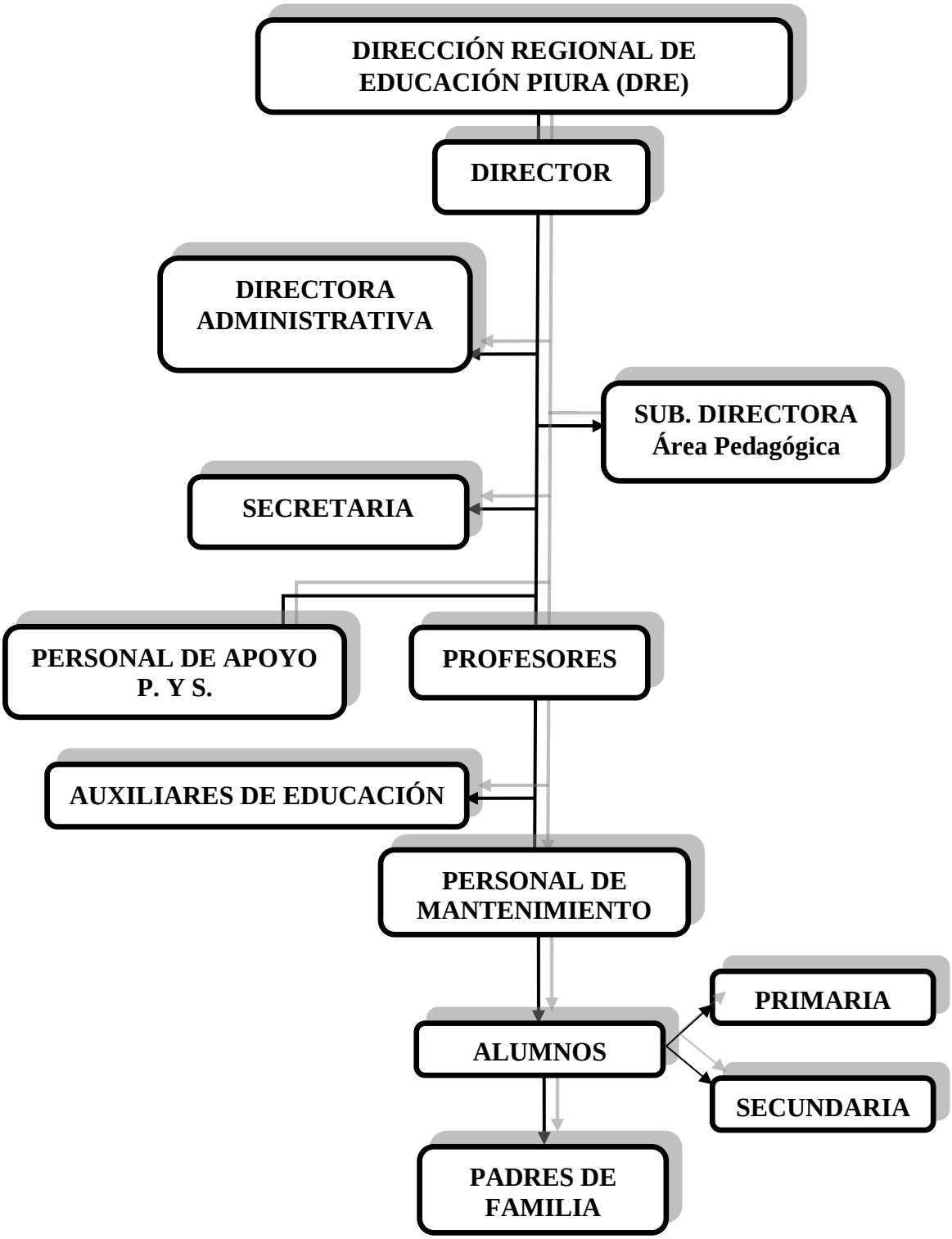
Tabla Nro. 02: Resumen Software I.E. San Miguel Arcángel

SOFTWARE	
Tipo/Clase	**Versión**
Microsoft Office	2010,2013
Adobe Photoshop	2016
Google Chrome	52.0.7
Antivirus ESET NOD32	2015
WINRAR	12
Sistema Operativo Windows	7 , 8

Fuente: Elaboración Propia.

Organigrama

Gráfico Nro. 04: Organigrama de la Institución Educativa



Fuente: I.E. San Miguel Arcángel

2.2.3. TIC en las Instituciones Educativas del Perú

Las herramientas TIC son un gran potencial en la educación, ya que ha estimulado el desarrollo y la investigación en diversos sistemas de enseñanza aprendizaje, los cuales, además de proporcionar material educativo multimedia, permiten clasificar, evaluar y orientar las actividades de los alumnos para que estos aprendan eficientemente y que los docentes puedan adquirir a información necesaria para educarlos de una buena manera. Muchas Instituciones Educativas utilizan las TIC para brindar educación no presencial dentro de su mismo campus. Es importante considerar que este tipo de educación implica un cambio cualitativo dentro de las instituciones educativas, pero lo más importante es la calidad del aprendizaje de los alumnos y la seguridad informática que deberán de tener. En el Perú existen actualmente 45.000 centros educativos públicos y más de seis millones de alumnos. Además, las planillas del Estado cuentan con 342.949 docentes. Dentro de las tecnologías que apoyan el aprendizaje se encuentran los llamados "Programas educativos" (Educación software), término que se ha empleado genéricamente para involucrar muchos tipos de aplicaciones con objetivos y usos diferentes. El aprendizaje del alumno es completamente libre puesto que no existen guías de estudio, aunque podemos encontrar ambientes adaptativos en donde el aprendizaje es guiado a través de recomendaciones o sugerencias (23).

2.2.4. Tecnologías de Información y Comunicación (TIC)

Las TIC son aquellas herramientas que reúnen los elementos y las técnicas usadas en el tratamiento, procesamiento y transmisión de la información, enfocadas a dar soluciones a las necesidades de la sociedad. Las TIC se han integrado a la sociedad, tomando importancia al permitir disminuir la brecha digital y social; las TIC tienden a tomar un lugar creciente en la vida humana y el funcionamiento de las sociedades. A pesar de los importantes avances en este campo aún debemos afianzar el rol transformador que las TIC deberán tener dentro de las agendas de los diferentes sectores públicos y privados. Las políticas públicas dirigidas al desarrollo de la economía digital se han concentrado en aspectos de infraestructura y no han podido ser desarrolladas en otros aspectos. Por otro lado los sectores privados TIC necesitan mejorar su nivel de articulación y presencia que un sector de esta naturaleza debería tener en la sociedad Peruana (24).

En los últimos años se han presentado grandes cambios como la apertura de mercado y no solo de esta sino también en la educación. Esta apertura de las herramientas TIC ha fomentado un ambiente de competencia en el cual las nuevas tecnologías son parte fundamental de nuevas estrategias competitivas; es por ello que antes pensábamos en una educación formal, hoy en día solo nos dedicamos a buscar una organización que brinde una buena educación pero a manera tecnológica en donde ningún usuario es ajeno a esto; para ello es necesario la tecnología y la forma en que esta es utilizada (25).

Las TIC hoy en día están abarcando todas las áreas de la sociedad, especialmente en el ámbito de la educación, ya que alumnos y docentes son beneficiados por ellas, pero así como cualquier

herramienta de apoyo tiene ventajas y desventajas por lo que veremos a continuación:

El Financiero (26) muestra un artículo donde menciona que estas tecnologías tienen un efecto multiplicador en los mercados, debido a que todos los sectores económicos las utilizan como herramientas de operaciones y de productividad para ser más eficientes, actualmente representan el 7 por ciento del Producto Interno Bruto (PIB) global. A nivel macroeconómico, por cada 10 por ciento de aumento en la penetración de banda ancha, el PIB crece en 1.3 por ciento, sin tomar en cuenta el efecto multiplicador que tienen como propulsoras de desarrollo en educación, salud, bienestar y entretenimiento, de acuerdo con datos del Banco Mundial. Las TIC también tienen sus ventajas y desventajas las cuales mostraremos a continuación:

Ventajas

- Interacción a través de foros o Redes Sociales.
- Diversificación de internet.
- Aprendizaje propio a manera de cursos online.
- Desarrollar habilidades.
- Corrección a alguna falla ortográfica.

Desventajas

- Distracción
- Aprendizaje Superficial
- Proceso educativo poco humano
- No todos aprenden con los cursos online
- Puede anular habilidades y capacidad crítica

2.2.5. Las TIC en la Educación

En los últimos años el avance de las Tecnologías de Información y Comunicación, ha impactado la educación por lo que se están planteando nuevos requerimientos en los planes de estudios a nivel mundial, creando nuevos procesos o métodos de enseñanza (10).

Echeverría (27), nos dice que las nuevas tecnologías (redes de computadoras, satélites, televisión por cable, multimedia, hipermedia, Internet, telefonía móvil, videoconferencia, entre otros) no sólo afectan la transformación de las tareas que se realizan con ellas, sino que también tienen consecuencias sobre la forma de percibir el mundo, sobre las creencias y las maneras de relacionarse de los individuos, transformando sustantivamente la vida social y cotidiana de la misma no queda ajeno la educación también siendo altamente motivantes y eficientes para los alumnos en su aprendizaje pero solo ellos no se ven beneficiados sino también los docentes.

Este trabajo de investigación presenta algunas bases teóricas que sustentan el uso de las TIC en la Educación.

Mendoza y Riveros (25), nos dicen que la metodología empleada es de tipo cualitativo, basada en la indagación documental. Las teorías consultadas se interpretaron por inferencia deductiva, teniendo en cuenta algunas consideraciones relacionadas con:

1) La sociedad del conocimiento y la tecnología informatizada.

2) El aprendizaje en el contexto de la sociedad global.

3) La telemática y la globalización del conocimiento.

4) Los usos del computador en la educación.

Estas tecnologías a pesar de ayudar también afecta demasiado a los procesos de educación que la sociedad ha generado, actualmente la educación está centrado en diversos software didácticos, soportes multimedia, etc., dejando de lado lo formal, trabajar con las herramientas TIC ha demostrado ser dinámicas y de modo que motiva a los alumnos siendo eficaces en el logro de ciertos aprendizajes comparada con los procesos tradicionales de enseñanza, basados en la tecnología impresa (25).

Desde casi sus inicios de la Institución Educativa "San Miguel Arcángel", se vienen utilizando las TIC, las cuales son manejadas por los alumnos y docentes que entran y salen de la institución, sin aun saber cómo manejarlas adecuadamente. Hoy en día las escuelas se van aproximando a las tecnologías de la información y la comunicación de maneras muy diversas, negociando entre los avances mediáticos y tecnológicos, las culturas organizacionales, las necesidades de los docentes, las brechas generacionales, las apropiaciones autónomas de los alumnos y las expectativas de la comunidad.

Finalmente, los TIC proporcionan a los docentes, alumnos y personal administrativo un medio virtual para relacionarse con sus pares, presentando retos especiales para el desarrollo social.

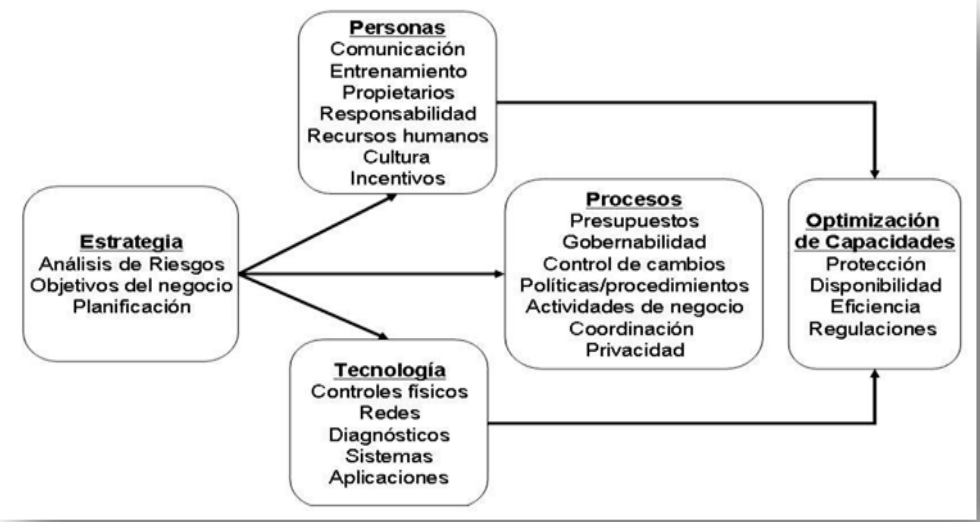
2.2.6. Seguridad informática

La seguridad informática es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma (14).

Espiñeira, Sheldon y Asociados (2), comentaron en una publicación en un sitio web, una definición de Seguridad informática o como también se le conoce “Seguridad informática”, refiriéndola como la “Encargada de Proteger los activos de Información de una organización contra pérdidas o el uso indebido de la misma, además de permitir el acceso a los activos de la información, dando apoyo a los objetivos de la organización”. Cabe agregar que la misma cumple un rol estratégico en los procesos de negocios identificando los recursos que deberán resguardarse o restringirse dentro una empresa, lo cual conlleva a mejorar las operaciones con clientes, socios, proveedores y empleados. En el gráfico siguiente, se muestra la relación de la seguridad informática en los recursos organizacionales.

La seguridad informática se ha vuelto una principal preocupación dentro de las empresas ya que el uso de las TIC, se ha vuelto cada vez más extenso en la sociedad, por lo que así como los activos a proteger y las vulnerabilidades han aumentado; por lo que los ciberataques se dan de manera consecutiva trayendo consigo consecuencias devastadoras como la revelación de información confidencial o la usurpación financiera de la empresa (2).

Gráfico Nro. 05: Estrategias



Fuente: Tomado y adaptado de Espiñeira, Sheldon y Asociados (2).

Por lo que podríamos decir que el concepto de seguridad informática no solo es de aspecto tecnológico, sino que es una solución integrada que ayudara a mantener la información de la organización a buen recaudo por lo que se deberán de contar con reglas, lineamientos, asignación de responsabilidades, además de incluir los procedimientos preestablecidos, y personal capacitado para la gestión del proceso (2).

Bossio y Gros (28), exponen que el término de la seguridad informática para sistemas de información, no es algo nuevo, existe desde hace tiempo, solo que ahora se encuentra en fase de evolución permanente debido a los avances técnicos en materia informática. Los autores expresan que los avances de la actualidad, en el que se destaca, el auge de la globalización y la apertura de las telecomunicaciones; los riesgos y las amenazas aumentan en forma

alarmante. En este orden de ideas, la seguridad informática o de la información se basa en 3 pilares fundamentales, como son:

- **Confidencialidad:** Es el aseguramiento de que la información, no es accesada por personas o entidades no autorizadas.
- **Integridad**: garantiza que la información es creada, modificada, o eliminada solo por el personal autorizado.
- **Disponibilidad:** Los datos o la información estarán al momento y en la forma en la que son requeridos por el personal autorizado.

Los autores hablan de un principio que tiene relación con la aceptación/no aceptación debido a los avances tecnológicos, este principio se basa en la aceptación de un mensaje y en la constancia de envió del mismo, este proceso se realiza a través de seguimientos electrónicos y la utilización de certificados o firmas digitales, ya que así se asegura que todo mensaje tenga un origen y un destino confiable.

Ventajas

- Reduce el Riesgo de pérdida de la información de la organización.
- Mantiene la confidencialidad de la información.
- Asegura integridad y confiabilidad de los datos.
- Asegura la disponibilidad de la información.
- Asegura el cumplimiento de las leyes de seguridad nacionales para la seguridad informática de las organizaciones cumpliendo las reglas propuestas.

Así como tiene ventajas para las organizaciones es muy importante tener su información a buen recaudo, pero no debes de ignorar que esto también tiene sus desventajas las cuales mencionaremos a continuación:

- Comunicaciones más lentas (Por el uso de algoritmos de Encriptación de Datos, uso de Firewalls, por lo que las hace más lentas).
- Molestia de los empleados por nueva normativa para el uso de la información, acceso al hardware, software, etc.
- Olvido de contraseñas, debido a los frecuentes cambios.

Laundon (29), hace mención a algunos argumentos que podrían presentarse al momento de que se establezcan políticas o procedimientos para la seguridad informática o planes de seguridad informática. Explica que "La construcción de los mecanismos de control para un sistema de información pueden ser muy costosos y complicados para su empleo, lo que no es económico y tampoco operativamente factible". Es preciso que la organización realice un análisis de la relación costo/beneficio y determine los mecanismos de control que le ofrezcan la protección más eficiente, sin necesidad de reducir eficiencia operativa y sin incrementar gastos en el presupuesto.

La Oficina Nacional de Gobierno Electrónico e Informática-ONGEI (30), nos muestra la facilidad para el acceso a información y comunicación, por el uso generalizado de las redes abiertas, como Internet, y de la telefonía celular nos genera grandes cambios en las actividades de las personas y en diversos sectores, como son la educación, el trabajo, la administración pública, la industria y el

comercio, llegando incluso a trasformar las formas de las relaciones humanas y sociales.

En las instituciones es importante contar con la Seguridad informática ya que cualquiera puede obtener esta y llevarla a la competencia por lo que la Institución Educativa “San Miguel Arcángel”, requiere que su información tenga una buena seguridad, y este a buen recaudo.

2.2.7. Seguridad informática en las TIC

La seguridad informática se enfoca en la protección de la infraestructura tecnológica, para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes, las cuales permiten minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas siendo este tipo de información como información privilegiada o confidencial (31).

Dado que Internet es verdaderamente global, ningún secreto de valor debería ser comunicado a través de ella sin la ayuda de la criptografía. En el mundo de los negocios, información como números de tarjetas de crédito, autenticaciones de clientes, correos electrónicos e incluso llamadas telefónicas acaba siendo enrutada a través de Internet. Ya que gran parte de esta información corporativa no debe ser escuchada por terceras personas, la necesidad de seguridad es obvia. Sin embargo, la Seguridad en Internet no es sólo una preocupación empresarial. Toda persona tiene derecho a la privacidad y cuando ésta accede a Internet su necesidad de

privacidad no desaparece. La privacidad no es sólo confidencialidad, sino que también incluye anonimato (3).

2.2.8. Agresiones a la Seguridad informática

Aldana (31), hace mención a los tipos de agresión a la seguridad de un sistema de computadores o de redes se caracterizan mejor observando la función del sistema como proveedor de información. En general, existe un flujo de información desde un origen, como puede ser un fichero o una región de memoria principal, a un destino, como otro fichero o un usuario. Hay cuatro tipos de agresión:

- **Interrupción:** Se da cuando un recurso del sistema se destruye o no llega a estar disponible o se inutiliza. Ésta es una agresión de disponibilidad. Ejemplos de esto son la destrucción de un elemento hardware (un disco duro), la ruptura de una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

- **Intercepción:** Se da cuando un ente no autorizado consigue acceder a un recurso. Ésta es una agresión a la confidencialidad. El ente no autorizado puede ser una persona, un programa o un computador. Ejemplos de agresiones a la confidencialidad son las intervenciones de las líneas para capturar datos y la copia ilícita de ficheros o programas.

- **Modificación:** Se da cuando un ente no autorizado gana acceder y realiza modificaciones que deterioran el recurso. Ésta es una agresión a la integridad. Algunos ejemplos son los cambios de valores en un fichero de datos, alterando un programa para que funcione de una forma diferente, y

modificando el contenido de los mensajes que se transmiten en una red.

- **Fabricación:** Se da cuando una parte no autorizada introduce objetos falsos en el sistema. Esta es una agresión a la autenticidad. Un ejemplo sería la incorporación de registros a un fichero.

2.2.9. Riesgos

La red puede estar expuesta a posibles causas que perjudican las conexiones de los equipos, a la vez puede estar en peligro la información que esta contiene en el almacenamiento, los posibles riesgos se dan mediante los siguientes bienes:

- Personal
- Hardware
- Software y utilitarios
- Datos e Información
- Documentación
- Suministro de Energía Eléctrica
- Suministro de Telecomunicaciones

Existen distintas clases de riesgo como lo son:

- Incendio
- Robo común y divulgación de la información
- Vandalismo
- Fallas en los equipos
- Equivocaciones
- Acción de Virus Informático
- Fenómenos naturales

- Accesos no Autorizados
- Manipulación y Sabotaje

2.2.10. Importancia de la Seguridad informática en las TIC.

La importancia de la seguridad en las TIC es algo que no se puede negar. La nueva sociedad de la información está en continua expansión y cada vez más datos se comparten en la red, muchos de ellos privados y de vital importancia para particulares o para empresas. Una falta de seguridad en las TIC que emplee una empresa puede llevarle a obtener perdidas millonarias y sufrir graves perjuicios tanto a nivel económico como a nivel social. Esto se debe a que además de las pérdidas económicas que pueda sufrir, su imagen se ve seriamente dañada al no presentar sistemas de seguridad en las TIC fiables, perdiendo la confianza de sus clientes. Por tanto, es imprescindible tener siempre en cuenta la importancia de la seguridad en las TIC especialmente en el mundo empresarial. Algunos de los ejemplos más sonados últimamente de la importancia de cuidar la seguridad en las TIC son los casos de Sega, Sony, Nintendo o Citibank. En el caso de las compañías dedicadas a la industria de los videojuegos, han sufrido respectivos ataques informáticos en los que los hackers sortearon la seguridad en las TIC y obtuvieron información privada sobre más de 100 millones de clientes, referente a nombre, dirección, claves de acceso, etc. El caso de Citibank es aún más grave, se estima que el ataque logró acceder a las cuentas de unos 3.400 clientes, tomando unos 800 euros de promedio da cada una de las cuentas, poniendo en evidencia los sistemas de seguridad TIC del banco. Observando estos datos, podemos entender la importancia de la seguridad informática en las TIC incluso en pequeños negocios que operen en Internet, ya sea para ofrecer sus productos y servicios para realizar trámites con el banco. Por ello, que para la Institución

Educativa será imprescindible formarse al respecto para contar con los sistemas de seguridad más eficientes y evitar estos problemas, realizando un master executive en seguridad en las comunicaciones y la información (3).

2.2.11. Normativas de Seguridad

Existen diversas normativas de seguridad que las organizaciones actualmente implantan para la seguridad de la información. Estas normativas están diseñadas para perseguir un solo objetivo incluyendo todos los departamentos que son parte de la estructura de la organización para poder obtener una buena seguridad, teniendo como finalidad presentar lineamientos que son necesarios para la organización y se pueda implantar (12).

2.2.12. ISO 27001

La ISO/IEC 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO), la que a su vez describe cómo gestionar la seguridad informática adecuada en una empresa. ISO/IEC 27001 puede ser implementada en cualquier tipo de organización, la misma que a su vez puede ser, con o sin fines de lucro, privada o pública, pequeña o grande. Está norma está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. La norma ISO 27001 define cómo organizar la seguridad de información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información (32).

La ISO 27001 es para la seguridad de información lo mismo que la ISO 9001 es para la calidad: es una norma redactada por los mejores especialistas del mundo en el campo de seguridad informática y su objetivo es proporcionar una metodología para la implementación de la seguridad informática en una organización (14).

La certificación ISO 27001 avala la adecuada implantación, gestión y operación de todo lo relacionado con la implantación de un SGSI, siendo la norma más completa que existe en lo relativo a la implantación de controles, métricas e indicadores que permiten establecer un marco adecuado de gestión de la seguridad informática para las organizaciones.

2.2.13. Definición de Políticas de Seguridad

Las políticas y normas son el instrumento que adopta la empresa para definir las reglas de comportamiento aceptables. La seguridad informática y el modo de tratarla no es una excepción, por lo que las políticas son reglas y prácticas que regulan la manera en que se deberán dirigir, proteger y distribuir los recursos en una organización para llevar a cabo los objetivos de seguridad informática de la misma. Desde que se realiza la planificación de las políticas de seguridad es necesario contar con personal responsable que da seguimiento al proceso de definición de estas. Ya que deben ser creada de manera clara que vayan acorde a la misión, recursos, tipo de red, usuarios entre otros (33).

2.2.14. Políticas de Seguridad Informática

Las políticas de seguridad informática tienden a establecer medidas de índole técnica e institucional, siendo las más

indispensables en la calidad de la seguridad de las TIC, consigo las personas que tienen interacción con los equipos tecnológicos.

En una institución puede tener muchas áreas y estas contar con sus propias redes y más si la organización es grande cada uno puede contar con diversos administradores, caso contrario que los sitios no cuenten con redes cada uno puede tener sus políticas de seguridad de red, pero sin embargo los sitios se encuentran conectados mediante una red interna, por lo cual se deberán de tomar cada uno de los objetivos interconectados (6).

Llamamos sitio a los lugares donde las organizaciones cuentan con computadoras y demás relacionado a las redes como podrían ser:

- Estaciones de Trabajo
- Computadoras, host y servidores
- Dispositivos de interconexión Gateway, routers, bridges, repetidores
- Servidores de terminal
- Software para conexión de red y aplicaciones
- Cables de red
- La información de archivos y bases de datos

Al implementarse la política de seguridad de red esta debe de tener en cuenta todos los recursos, considerando las necesidades y requerimientos de seguridad para todas las redes interconectadas. Es importante idear una política de seguridad que respalde los intereses, por ejemplo seria el uso deliberado de direcciones IP, detrás de Gateway de las firewall que ya están siendo usadas por alguien más. En este los ataques que se hicieran contra su red mediante la falsificación de las direcciones IP, se desviaran a la organización a la que pertenecen las direcciones IP que se están usando (17).

2.2.15. Objetivo de una política de seguridad

El objetivo de una política de seguridad informática es la de implantar una serie de leyes, normas, estándares y prácticas que garanticen la seguridad, confidencialidad y disponibilidad de la información, y a su vez puedan ser entendidas y ejecutadas por todos aquellos miembros de la organización a las que van dirigidos (33).

Álvarez (34), nos dice que es importante tener una política de seguridad de red ya que permitirá proteger sus redes de información delicada y/o secretos importantes de personas que quieran acceder al sistema de manera ilegal. Actualmente tener una política de seguridad de red nos permite, asegurar, que los esfuerzos dedicados a la seguridad impliquen un costo razonable. Esto significa que usted debe conocer cuales recursos vale la pena proteger, y cuales son más importantes que otros. También debe identificar la fuente de amenazas de la que usted está protegiendo a los recursos de la red. A pesar de toda la publicidad acerca de los intrusos que irrumpen en una red, muchos estudios indican que, en

el caso de la mayoría de las organizaciones, las verdaderas pérdidas causadas por los usuarios internos son mucho mayores.

2.2.16. Principios fundamentales de las políticas de seguridad

Los principios fundamentales son: responsabilidad individual, autorización, mínimo privilegio, separación de obligaciones, auditoría y redundancia. Son las ideas principales a partir de las cuales son diseñadas las políticas de seguridad (34).

- **Responsabilidad individual:** Este principio da a entender que cada persona dentro de la institución es responsable de cada uno de sus actos, aun si tiene o no conciencia de las consecuencias.

- **Autorización:** Este principio indica que sebe de seguir las reglas explícitas acerca de quién, como, cuando y de qué manera puede utilizar los recursos.

- **Mínimo privilegio:** Este principio indica que cada miembro debe estar autorizado a utilizar únicamente los recursos necesarios para llevar a cabo su trabajo. Además de ser una medida de seguridad, también facilita el soporte y mantenimiento de los sistemas.

- **Separación de obligaciones:** Las funciones deberán ser divididas entre las diferentes personas relacionadas a la misma actividad o función, con el fin de que ninguna persona cometa un fraude o ataque sin ser detectado. Este principio junto con el de mínimo privilegio hacen que las posibilidad de ataques a la seguridad se reduzcan, pues los usuarios sólo pueden hacer uso de los

recursos relacionados con sus actividades, además de que facilita el monitoreo y vigilancia de usuarios, permitiendo registrar y examinar sus acciones.

- **Auditoría:** Todas las actividades, sus resultados, gente involucrada en ellos y los recursos requeridos, deberán ser monitoreados desde el inicio y hasta después de ser terminado el proceso. Además es importante considerar que una auditoría informática busca verificar que las actividades que se realizan así como las herramientas instaladas y su configuración son acordes al esquema de seguridad informática realizado y si éste es conveniente a la seguridad requerida por la empresa.

- **Redundancia:** Este principio se basa principalmente sobre las copias de seguridad informática, estas deberán de ser creadas múltiples veces en determinados tiempos si estas se realizan frecuentemente es mucho mejor y deben ser almacenados en lugares distintos. Sin embargo, la redundancia como su nombre lo indica, busca "duplicar" y en este sentido se puede decir que a través de los respaldos se duplica información, y lo mismo se puede realizar en diferentes aspectos, como por ejemplo: en cuanto a energía eléctrica, una planta de luz para garantizar que opere en casos de emergencia, servidores de datos que entren en operación cuando el primario sufra una avería, etcétera, de manera tal que la redundancia se considera en aquellos casos o servicios que se vuelven imprescindibles para la institución y que no pueden suprimirse pase lo que pase.

2.2.17. Como plantear una política de seguridad

Para poder definir una política de seguridad de red debemos de analizar e indagar para así poder elaborar los procedimientos y planes para poder respaldar los archivos contra perdida y daño, debemos de realizarnos las preguntas (34):

- ¿Qué recursos está usted tratando de proteger?
- ¿De quienes necesita proteger los datos?
- ¿Qué tan posibles son las amenazas?
- ¿Qué tan importante es el recurso?
- ¿Qué medidas puede implementar para proteger sus bienes de forma económica y oportuna?
- Examine periódicamente su política de seguridad de red para ver si han cambiado los objeticos y circunstancias de la red.

Debemos tener en cuenta que el diseño de la política de seguridad se debe de ver la gente que participara en ella.

2.2.18. Parámetros para establecer Políticas de Seguridad Informática (PSI)

La implementación de Políticas de Seguridad informática es un proceso técnico y administrativo que comprende a toda la institución por ende, debe estar avalado y contar con un fuerte apoyo de la dirección, ya que sin el apoyo de esta, su

implementación será más compleja en algunos casos puede fracasar. Es importante cuando se realicen las políticas de seguridad informática que se consideren por lo menos los siguientes aspectos (33):

- Se debe de realizar un completo análisis de riesgos informáticos, para así identificar los problemas que se están dando poder adecuar las políticas a la realidad de la institución.
- Reunirse con los encargados donde se encuentran los equipos tecnológicos, ya que ellos tienen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.
- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, con ello informar sobre los beneficios y riesgos relacionados con los recursos tecnológicos, y sus elementos de seguridad.
- Se debe de identificar quién tendrá la máxima autoridad para la toma de decisiones en los equipos tecnológicos, pues esta debe ser la más interesada en proteger los activos críticos de la institución.
- Se debe de realizar un monitoreo periódico de los procedimientos y operaciones que realice la institución, de forma tal, que ante cambios las políticas puedan ser actualizadas oportunamente.
- Se debe detallar de manera explícita y concreta el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.
- Las políticas de seguridad deben de ser revisadas y actualizadas cada dos años de acuerdo a lo que se

necesite, revisada y aprobada por el encargado del área de informática.

El problema de implantarse una política de seguridad está en el escaso conocimiento que se dan en las empresas por lo que se debe ser capaz de convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática, sino los esfuerzos de su implementación pueden ser desperdiciados (35).

2.2.19. Violaciones a la Política de Seguridad

Las violaciones en la política de seguridad generan grandes pérdidas de información dentro de una organización, ya que estas son de suma importancia. Estas violaciones son cometidas tanto por usuarios externos a través de la red, como también lo puede realizar un usuario de la misma organización generando un quiebre institucional. Distinguiéndose entre ellos el límite de acceso a la red, administrativo, legal o político, si son violadas se toma acciones según el tipo delito que se ha ocasionado en la red. La definición del tipo de violación llega a ocasionar grandes problemas externos e internos de acuerdo a las advertencias políticas legales de la misma institución. Por lo que las políticas de seguridad que da la institución deberán darse a conocer para los usuarios internos, en este caso sean docentes, alumnos y personal administrativos. Al presentar un documento de políticas de seguridad estas deberán tener procesos para el manejo de diversos problemas de violación, por lo que debe tenerse un registro de accesos a la red que se deberán de verificar periódicamente, analizando y buscando la actualización de la política de seguridad que se haya originado (36).

2.2.20. Prevenir una violación a la Política de Seguridad

Para prevenir una violación los administradores de la política de seguridad siempre deberán de estar atentos a los diferentes tipos de cambios, que hacen que la información de la institución se encuentre vulnerable a cualquier problema permitiendo que la política sea actualizada y generando un bloqueo automático en la red ya que si este no es detectado de inmediato puede generar grandes pérdidas a la hora de restablecerla, al igual para cada integrante de la institución si se genera una violación a las políticas de seguridad establecidas se debe de informar al encargado de informática para que pueda generar un control en cuanto a lo que se esté generando sin demora, por lo que la violación pone el riesgo y la integridad de las personas (36).

2.2.20. Concientización

Las políticas de seguridad establecidas, tanto como estándares y guías dentro de la institución deben ser informadas a la población que se encuentra dentro de la institución para que puedan tener en cuenta sus responsabilidades y que no se pueda ver afectada la seguridad informática. Al concientizar a la población en general se debe brindar las normas, requerimientos entre otros, así como todo tipo de consecuencia que puede haber si no se cumplen con estas. Brindándoles folletos y sobre todo un manual donde ellos puedan tener la información adquirida en cuanto a la seguridad informática que se debe tener, llevarlos a tener un debate sobre qué hacer y no hacer en el área de informática y como darle un buen uso a las TIC (12).

III. HIPÓTESIS

La propuesta de implementación de seguridad informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016, mejorará el control de riesgos informáticos.

IV. METODOLOGÍA

4.1. Tipo de la Investigación

Por las características de la investigación, el presente trabajo es de enfoque cuantitativo ya que reúne las condiciones metodológicas de una investigación aplicada, en razón, que se utilizan conocimientos fundamentales sobre la Seguridad Informática en las Tecnologías de Información y Comunicación, a fin de aplicarlas a la I.E. San Miguel Arcángel.

Sampieri, Collado y Lucio (37), en su informe nos dice que una investigación es de enfoque cuantitativo cuando se utiliza la recolección y el análisis de datos para contestar preguntas de investigación y probar hipótesis establecidas previamente, y confiando en la medición numérica, el conteo y frecuentemente en el uso de la estadística para establecer con exactitud patrones de comportamiento en una población.

4.2. Nivel de la Investigación

De acuerdo a la naturaleza de la investigación, reúne por su nivel, las características de una investigación descriptiva.

Ávila (38), menciona en su libro que el propósito del investigador es describir situaciones y eventos. Esto es, decir cómo es y se manifiesta determinado fenómeno. Los estudios descriptivos buscan especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis, midiendo o evaluando diversos aspectos, dimensiones o componentes del fenómeno o fenómenos a investigar. Por lo que su meta no se limita a la recolección de datos, sino a la predicción e identificación de las relaciones que existen entre dos o más variables.

4.3. Diseño de la Investigación

El diseño de la investigación es no experimental y de corte transversal, ya que es aquella que se realiza sin manipular deliberadamente variables. Se basa fundamentalmente en la observación de fenómenos tal y como se dan en su contexto natural para analizarlos con posterioridad. En el tipo de investigación no experimental no hay condiciones ni estímulos a los cuales se expongan los sujetos del estudio. Los sujetos son observados en su ambiente natural. Y es transversal ya que se recolectan datos en un solo momento, en un tiempo único. Su propósito es describir variables, y analizar su incidencia e interrelación en un momento dado (39).

Por lo que el gráfico es el siguiente:

M =Muestra

O = Observación

4.4. Población y Muestra

a) Población

Arias (40), señala que la población "es el conjunto de elementos con características comunes que son objetos de análisis y para los cuales serán válidas las conclusiones de la investigación". Por lo que para el desarrollo de esta investigación, se necesitó realizar un estudio de la población de la institución. Por lo consiguiente, la población de la presente investigación estará constituida por el total de 1463 personas afectadas de la I.E. San Miguel Arcángel. La población ha quedado delimitada en 60 personas que nos serán de ayuda en la investigación.

b) Muestra

La muestra está conformada por las 60 personas delimitadas de la población las cuales están involucradas docentes, alumnos y personal administrativo de la I.E. San Miguel Arcángel.

Tabla Nro. 03: Muestra a utilizar

ÁREA	CANTIDAD
Alumnos de 5to "A"- nivel Secundario	30
Docentes que más que utilizan las TIC.	20
Directora	01
Secretaria	01
Personal administrativo(administrador y coordinadores)	05
Mantenimiento	03
TOTAL	**60**

Fuente: "Elaboración propia"

4.5. Definición y Operacionalización de variables e indicadores

Tabla Nro. 04: Definición Operacional de Variables de Estudio

Variable independiente	Definición conceptual	Dimensiones	Indicadores	Definición operacional
Propuesta de Implementación de Seguridad Informática en las TIC	**Tecnologías de información y Comunicació**n: Son aquellas herramientas que reúnen los elementos y las técnicas usadas en el tratamiento, procesamiento y transmisión de la información, enfocadas a dar soluciones a las necesidades de la sociedad (24). **Seguridad informática:** es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma (14).	Nivel de satisfacción con respecto a la Seguridad Informática en las TIC.	Seguridad confiable en los equipos tecnológicos. Seguridad eficiente y eficaz al guardar información.	La I.E San Miguel Arcángel cuenta con herramientas TIC, estas interactúan con docentes, alumnos y personal administrativo, por lo que requiere de seguridad informática en ellas cuya eficacia se evaluara mediante capacitaciones e implementación de políticas de seguridad.
		Nivel de satisfacción con respecto a la formación y capacitación a los Docentes y Alumnos sobre el manejo de las TIC.	Manejo de las TIC. Formación en el uso de las TIC.	
		Nivel de satisfacción con respecto a las TIC en el proceso de enseñanza aprendizaje.	TIC en clases. Interacción con los alumnos y docentes.	

Fuente: Elaboración Propia

4.6. Técnicas e instrumentos de recolección de datos

Observación directa: con esta técnica se podrá tener una percepción más clara del problema planteado, pudiendo observar la situación desde el enfoque de los usuarios como de los integrantes de la administración. Se obtendrá un mejor entendimiento acerca de los problemas actuales y de la acción que se debe tomar para solucionarlos.

Encuestas: esta técnica será aplicada de manera escrita, y con ella se recolectará información valiosa de parte de los usuarios para optimizar el diagrama e infraestructura tecnológica.

Procedimiento de Recolección de Datos: Se seleccionara a las personas adecuadas para poder aplicar las encuestas, de manera apropiada, por medio de visitas a las diferentes áreas de la Institución Educativa.

4.7. Plan de Análisis

Obtenidos los resultados, se crearan tablas en el programa Excel, procediéndose a realizar los gráficos de los mismos; a través del cual se obtuvo las frecuencias, realizándose luego el análisis de distribución de dichas frecuencias con sus respectivas figuras.

4.8. Matriz de Consistencia

Tabla Nro. 05: Matriz de Consistencia

Título: Estudio de las Tecnologías de Información y Comunicación para la Seguridad informática de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	METODOLOGÍA
PROBLEMA ¿Es necesario determinar el estudio de la seguridad informática en las TIC de la I.E San Miguel Arcángel, Catacaos - Piura; 2016?	**OBJETIVO GENERAL** Proponer la implementación de Seguridad informática en las TIC de la I.E. San Miguel Arcángel en el año 2016 **OBJETIVOS ESPECÍFICOS** 1. Identificar el estudio de la Seguridad Informática existente dentro de la I.E San Miguel Arcángel.	La propuesta de implementación de seguridad informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016, mejorará el control de riesgos informáticos.	Propuesta de Implementación de Seguridad Informática en las TIC	Tipo: Cuantitativo Nivel: Descriptivo Diseño: No Experimental Corte Transversal Muestra:

	2. Evaluar los diferentes efectos del manejo de las herramientas TIC en la I.E. San Miguel Arcángel. 3. Comparar los diferentes dominios o áreas que se deberán tomar en cuenta según las mejores prácticas con el fin de formular estrategias para la seguridad Informática en la I.E. San Miguel Arcángel. 4. Desarrollar una buena metodología basada en las mejores prácticas para que cualquier organización pueda desarrollarlo teniendo una seguridad Informática de alta calidad con las políticas establecidas.			60 (Docentes, Alumnos y Personal Administrativo) Técnica: Encuesta Instrumento: Cuestionario

Fuente: Elaboración Propia

4.9. Principios Éticos

Durante el desarrollo de la presente investigación denominada "Propuesta de implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, se ha considerado estrictamente cumplir con los principios éticos permitiendo que la investigación realizada tenga originalidad como también se ha respetado los derechos de propiedad intelectual de los libros de textos y fuentes electrónicas que facilitaron el manejo de la estructura del trabajo de investigación.

De la misma forma se puede decir que los datos que han sido utilizados son públicos, ya que estos son conocidos por más personas y son aplicados en diversos trabajos de investigación sin estar restringidos, incluyendo contenido sin modificaciones excepto en pequeñas partes que se utilizaron para complementar el contenido de la metodología para realizar un buen análisis.

Mientras que el contenido de la recopilación de información se dio referente a las encuestas aplicadas a los docentes, alumnos y personal administrativo, por otro lado, se conserva el contenido de las respuestas, manifestaciones y opiniones recolectadas, estableciendo la relación causa-efecto de las variables de investigación, siendo realizado de manera anónima para así lograr objetividad en los resultados.

V. RESULTADOS

5.1. Resultados

A. Dimensión 01: NIVEL DE SATISFACCIÓN CON RESPECTO A LA SEGURIDAD INFORMÁTICA EN LAS TIC

Tabla Nro. 06: Implementación de Seguridad Informática

Distribución de frecuencias y respuestas relacionadas a la implementación de Seguridad Informática en el ambiente de trabajo con las TIC, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	n	%
SI	06	10.00
NO	54	90.00
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Cree usted que la implementación de seguridad informática en las TIC es la adecuada en su ambiente de trabajo?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 06 se observa que el 90.00% de los docentes, personal administrativo y alumnos encuestados expresaron que la implementación

de Seguridad informática en las TIC que se maneja NO es la más adecuada en su ambiente de trabajo, mientras que el 10.00% indica que SI lo es.

Tabla Nro. 07: Ubicación de Equipos Informáticos

Distribución de frecuencias y respuestas relacionadas a la ubicación de los equipos informáticos dentro de la I.E., para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	14	23.30
NO	46	76.70
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Usted cree que los ambientes donde se encuentran los equipos informáticos dentro de la institución son seguros?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 07 se puede decir que el 76.70% de los docentes, personal administrativo y alumnos encuestados opinaron que NO creen que los ambientes donde se encuentran los equipos informáticos dentro de la institución son seguros, mientras que el 23.30% indica que SI creen que son seguros.

Tabla Nro. 08: Uso de Antivirus

Distribución de frecuencias y respuestas relacionadas al uso de Antivirus necesario en los equipos informáticos, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	25	41.70
NO	35	58.30
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Considera que el uso de los antivirus en los equipos informáticos de la Institución son seguros cuando ingresa o retira información en algún dispositivo de almacenamiento?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 08 se expresa que el 58.30% de los docentes, personal administrativo y alumnos encuestados marcaron que NO consideran que el uso de los antivirus en los equipos informáticos de la Institución son seguros, mientras que el 41.70% indica que SI lo consideran.

Tabla Nro. 09: Seguridad y Confiabilidad de compartir archivos

Distribución de frecuencias y respuestas relacionadas a la seguridad y confiabilidad de compartir archivos por medio del internet, la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	20	33.30
NO	40	66.70
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Al navegar por internet, usted cree que existe la seguridad y la confiabilidad necesaria para compartir su información?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 09 se define que el 66.70% de los docentes, personal administrativo y alumnos encuestados formularon que al navegar por internet NO existe la seguridad y la confiabilidad necesaria para compartir su información, mientras que el 33.30% indica que SI existe.

Tabla Nro. 10: Ubicación de las Infraestructuras de las TIC críticas o con información

Distribución de frecuencias y respuestas relacionadas a la ubicación de las infraestructuras de las TIC críticas o con información sensible dentro de la institución, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	n	%
SI	19	31.70
NO	41	68.30
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿La infraestructura de las TIC críticas o con información sensible con la que cuenta la institución, están ubicadas en entornos protegidos y con controles de acceso?, para la Propuesta de Implementación de las Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 10 refiere que el 68.30% de los docentes, personal administrativo y alumnos encuestados opinaron que la infraestructura de las TIC críticas o con información sensible con las que cuenta la institución NO están ubicadas en entornos protegidos y con controles de acceso, mientras que el 31.70% indica que SI lo están.

Tabla Nro. 11: Medidas de Protección

Distribución de frecuencias y respuestas relacionadas a las medidas de protección que se deben de tomar de acuerdo a la Seguridad informática, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	44	73.30
NO	16	26.70
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y Alumnos encuestados respecto a la pregunta: ¿Cree que la seguridad informática de su institución es importante y deben de tomarse las medidas adecuadas de protección?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 11 señala que el 73.30% de los docentes, personal administrativo y alumnos encuestados definieron que SI creen que la seguridad informática es importante dentro de la institución por lo que se deberían de tomar las medidas adecuadas de protección, mientras que el 26.70% indica que NO lo considera.

Tabla Nro. 12: Política de Protección

Distribución de frecuencias y respuestas relacionadas a las medidas de protección que se deberán de tomar de acuerdo a la Seguridad informática, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	16	26.70
NO	44	73.30
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿En su institución educativa existe alguna política de protección de la información que haga que la seguridad sea eficaz, cuando se produce un intercambio electrónico de información?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 12 señala que el 73.30% de los docentes, personal administrativo y alumnos encuestados definieron que NO existe una política de protección de información que haga que la seguridad informática sea eficaz al producirse un intercambio electrónico, mientras que el 26.70% indica que SI existe.

Tabla Nro. 13: Protección Confiable

Distribución de frecuencias y respuestas relacionadas a la protección confiable de los ordenadores de la I.E, para la Propuesta de Implementación Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	09	15.00
NO	51	85.00
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Usted considera que la institución le brinda la seguridad y protección confiable al utilizar una de sus computadoras para evitar pérdida, daños y modificación de la información con la que usted trabaja?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 13 se precisa que el 85.00% de los docentes, personal administrativo y alumnos encuestados expresan que NO consideran que la institución les brinde la seguridad y protección confiable al utilizar una de las computadoras para evitar pérdida, daños y modificación de la información dentro de la I.E., mientras que el 15.00% indica que SI lo considera.

Tabla Nro. 14: Pérdida de Información

Distribución de frecuencias y respuestas relacionadas a la perdida de información de la institución, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	45	75.00
NO	15	25.00
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Cree usted que podría ocurrir un robo ocasionando pérdida o deterioro de su información la cual retrasaría o perjudicaría su trabajo?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 14 se reconoce que el 75.00% de los docentes, personal administrativo y alumnos encuestados expresan que SI sienten que podría ocurrir que un robo ocasione pérdida o deterioro de su información la cual retrase o perjudique su trabajo, mientras que el 25.00% indica que NO siente que pueda ocurrir perdida de información.

Tabla Nro. 15: Seguridad con las TIC

Distribución de frecuencias y respuestas relacionadas a la Seguridad informática a través de las TIC, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	n	%
SI	11	18.30
NO	49	81.70
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿En la institución educativa consideran las TIC para brindar una seguridad informática eficiente?, para la Propuesta de Implementación de Seguridad Informática en las TIC I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 15 se analiza que el 81.70% de los docentes, personal administrativo y alumnos encuestados expresan que la institución educativa NO considera las TIC para brindar una seguridad informática eficiente, mientras que el 18.30% expreso que SI consideran que les brinde la seguridad informática eficiente.

B. Dimensión 02: NIVEL DE SATISFACCIÓN CON RESPECTO A LA FORMACIÓN Y CAPACITACIÓN A LOS DOCENTES, PERSONAL ADMINISTRATIVO Y ALUMNOS SOBRE EL MANEJO DE LAS TIC.

Tabla Nro. 16: Conocimientos sobre las TIC

Distribución de frecuencias y respuestas relacionadas a los conocimientos que se requieren referente a las TIC, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	n	%
SI	07	11.70
NO	53	88.30
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Tiene conocimientos acerca de las herramientas TIC, en su institución?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 16 se define que el 88.30% de los docentes, personal administrativo y alumnos encuestados expresaron que NO tienen conocimientos sobre las TIC dentro de su institución, mientras que el 11.70% indica que SI lo tiene.

Tabla Nro. 17: Inversión en TIC

Distribución de frecuencias y respuestas relacionadas a la inversión en TIC dentro de la institución, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	13	21.70
NO	47	78.30
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Cree usted que la institución considera importante invertir en herramientas TIC?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 17 se puede decir que el 78.30% de los docentes, personal administrativo y alumnos encuestados opinaron que NO creen que la institución considere importante invertir en TIC, mientras que el 21.70% indica que SI lo considera.

Tabla Nro. 18: Nivel de las TIC

Distribución de frecuencias y respuestas relacionadas al buen nivel de las TIC, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	23	38.30
NO	37	61.70
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Es bueno el nivel de las TIC en su Institución Educativa?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 18 se expresa que el 61.70% de los docentes, personal administrativo y alumnos encuestados marcaron que NO es bueno el nivel de TIC dentro de la institución educativa, mientras que el 38.30% considera que SI lo es.

Tabla Nro. 19: Manejo de las TIC

Distribución de frecuencias y respuestas relacionadas a la seguridad y confiabilidad de compartir archivos por medio del internet, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	22	36.70
NO	38	63.30
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Usted considera que los docentes de la institución educativa tienen un buen manejo de las TIC?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 19 se define que el 63.30% de los docentes, personal administrativo y alumnos encuestados formularon que los docentes NO tienen un buen manejo de las TIC, mientras que el 36.70% indica que SI lo tienen.

Tabla Nro. 20: Información del gobierno para el manejo de las TIC

Distribución de frecuencias y respuestas relacionadas a la información que debería brindar el gobierno para el manejo de las TIC, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	n	%
SI	23	38.30
NO	37	61.70
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿El gobierno, informa de manera correcta a las instituciones educativas en cuanto al manejo de las TIC?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 20 se observa que el 61.70% de los docentes, personal administrativo y alumnos encuestados opinaron que el gobierno NO informa a las instituciones educativas en cuanto al manejo de las TIC, mientras que el 38.30% indica que SI lo hace.

Tabla Nro. 21: Temas Informáticos y Tecnológicos

Distribución de frecuencias y respuestas relacionadas a la capacitación frecuente en temas informáticos y tecnológicos, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	15	25.00
NO	45	75.00
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Su institución realiza capacitaciones frecuentemente en temas de informática y tecnología?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 21 señala que el 75.00% de los docentes, personal administrativo y alumnos encuestados definieron que su institución NO se realiza capacitaciones frecuentes en temas de informática y tecnología, mientras que el 25.00% indica que SI lo hacen.

Tabla Nro. 22: Capacitación para proteger su información

Distribución de frecuencias y respuestas relacionadas a la capacitación por parte del área de computación para proteger su información, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	26	43.30
NO	34	56.70
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Ha recibido capacitación útil por parte del área de computación de cómo proteger su información?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 22 señala que el 56.70% de los docentes, personal administrativo y alumnos encuestados definieron que NO han recibido capacitación útil por parte del área de computación de cómo proteger su información, mientras que el 43.30% indica que SI han recibido capacitación.

Tabla Nro. 23: Capacitación de Política de seguridad

Distribución de frecuencias y respuestas relacionadas a la capacitación de una política de protección dentro de la institución , para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	n	%
SI	24	40.00
NO	36	60.00
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿En la institución educativa existe una política de protección donde se les ha capacitado o formado en temas de seguridad informática a través de las TIC?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 23 se precisa que el 60.00% de los docentes, personal administrativo y alumnos encuestados expresan que en la institución educativa NO existe una política de protección donde se les ha capacitado o formado en temas de seguridad informática a través de las TIC, mientras que el 40.00% indica que SI existe y han recibido capacitación.

Tabla Nro. 24: Talleres de Seguridad informática

Distribución de frecuencias y respuestas relacionadas a la implementación de talleres referente a la Seguridad informática, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	20	33.30
NO	40	66.70
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿En su institución se implementan talleres de formación y preparación en temas seguridad y protección de información?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 24 se reconoce que el 66.70% de los docentes, personal administrativo y alumnos encuestados expresan en su institución NO se implementan talleres de formación y preparación en temas seguridad y protección de información, mientras que el 33.30% indica que SI los implementan.

Tabla Nro. 25: Tecnología actual

Distribución de frecuencias y respuestas relacionadas a la capacitación de temas actuales de informática y tecnología en la institución, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	n	%
SI	28	46.70
NO	32	53.30
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Siente que su institución se preocupa por capacitarlo en temas actuales de informática y tecnológicos? , para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 25 se analiza que el 53.30% de los docentes, personal administrativo y alumnos encuestados expresan que NO sienten que su institución se preocupa por capacitarlo en temas actuales de informática y tecnológicos, mientras que el 46.70% consideran que SI se preocupa por capacitarlos.

C. Dimensión 03: NIVEL DE SATISFACCIÓN CON RESPECTO A LAS TIC EN EL PROCESO DE ENSEÑANZA APRENDIZAJE.

Tabla Nro. 26: Implementación de las TIC

Distribución de frecuencias y respuestas relacionadas implementación de las TIC para un mejor rendimiento académico, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	n	%
SI	51	85.00
NO	09	15.00
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Considera usted que es necesaria la implementación de las TIC para un mejor rendimiento académico?, para la Propuesta de Implementación Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 26 se define que el 85.00% de los docentes, personal administrativo y alumnos encuestados se refirieron que SI es necesaria que la implementación de las TIC propiciara un mejor rendimiento académico, mientras que el 15.00% indica que NO lo considera.

Tabla Nro. 27: Clases con las TIC

Distribución de frecuencias y respuestas relacionadas al desarrollo de clases utilizando las TIC, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	08	13.30
NO	52	86.70
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿En su institución educativa se desarrollan las clases tomando en cuenta las herramientas TIC?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 27 se puede decir que el 86.70% de los docentes, personal administrativo y alumnos encuestados opinaron que en la institución educativa NO se desarrollan las clases tomando en cuenta las herramientas TIC, mientras que el 13.30% indica que SI las utilizan.

Tabla Nro. 28: Uso de las TIC en la práctica pedagógica

Distribución de frecuencias y respuestas relacionadas al uso de las TIC en la práctica pedagógica, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	19	31.70
NO	41	68.30
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Se incorpora el uso de TIC en la práctica pedagógica, mediante la aplicación de investigaciones actualizadas sobre educación y uso de tecnología como marco referencia?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 28 se expresa que el 68.30% de los docentes, personal administrativo y alumnos encuestados marcaron que NO se incorpora el uso de TIC en la práctica pedagógica, mediante la aplicación de investigaciones actualizadas sobre educación y uso de tecnología como marco referencia, mientras que el 31.70% expresan que SI las utilizan.

Tabla Nro. 29: Interacción de las TIC con los Alumnos

Distribución de frecuencias y respuestas relacionadas a la interacción de las TIC con los alumnos, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	n	%
SI	27	45.00
NO	33	55.00
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Considera que las TIC interactúan adecuadamente con los alumnos en el proceso de enseñanza?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 29 se define que el 55.00% de los docentes, personal administrativo y alumnos encuestados formularon NO consideran que las TIC interactúan adecuadamente con los alumnos en el proceso de enseñanza, mientras que el 45.00% indica que SI lo hace.

Tabla Nro. 30: Resultados y logros alcanzados con las TIC

Distribución de frecuencias y respuestas relacionadas a los resultados y logros alcanzados con las TIC actualizadas, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	20	33.30
NO	40	66.70
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Cree usted que se reflexiona respecto a los resultados y logros alcanzados en experiencias de aprendizaje desarrolladas con TIC actualizadas?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 30 se observa que el 66.70% de los docentes, personal administrativo y alumnos encuestados opinaron que NO se reflexiona respecto a los resultados y logros alcanzados en experiencias de aprendizaje desarrolladas con TIC actualizadas, mientras que el 33.30% indica que SI lo hacen.

Tabla Nro. 31: Seguimiento del proceso de aprendizaje bajo un rango de seguridad

Distribución de frecuencias y respuestas relacionadas al seguimiento del proceso de aprendizaje de los alumnos y teniéndolo bajo un rango de seguridad, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	n	%
SI	36	60.00
NO	24	40.00
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Se da seguimiento al proceso de aprendizaje de los alumnos utilizando las herramientas tecnológicas correspondientes y teniéndola bajo un rango de seguridad, dentro de su institución?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 31 señala que el 60.00% de los docentes, personal administrativo y alumnos encuestados definieron que SI se necesita dar seguimiento al proceso de aprendizaje de los alumnos utilizando las herramientas tecnológicas correspondientes y teniéndola bajo un rango de seguridad, mientras que el 40.00% indica que NO lo necesita.

Tabla Nro. 32: Seguridad informática en las TIC

Distribución de frecuencias y respuestas relacionadas a la seguridad informática en las TIC, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	17	28.30
NO	43	71.70
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Usted cree que la institución considera que el uso de las herramientas TIC son buenas en el proceso de aprendizaje, y que estas necesiten de la seguridad informática?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 32 señala que el 71.70% de los docentes, personal administrativo y alumnos encuestados definieron que NO cree que la institución considere que el uso de las herramientas TIC son buenas en el proceso de aprendizaje, y que estas necesiten en la seguridad informática, mientras que el 28.30% indica que SI lo cree.

Tabla Nro. 33: Herramientas y entornos de Trabajo

Distribución de frecuencias y respuestas relacionadas a las herramientas de aprendizaje y entornos de trabajo en la institución, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	n	%
SI	18	30.00
NO	42	70.00
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Se seleccionan estrategias de aprendizaje con uso de herramientas de productividad (Word, Excel, Power Point entre otros) y recursos de Internet para diseñar un entorno de trabajo con los alumnos?, para la Propuesta de Implementación de las Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 33 se precisa que el 70.00% de los docentes, personal administrativo y alumnos encuestados expresan que NO se seleccionan estrategias de aprendizaje con uso de herramientas de productividad y recursos de Internet para diseñar un entorno de trabajo con los alumnos, mientras que el 30.00% indica que SI lo hace.

Tabla Nro. 34: Recursos Tecnológicos

Distribución de frecuencias y respuestas relacionadas al uso de recursos tecnológicos a través de grupos de trabajo, para la Propuesta de Implementación de las Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	15	25.00
NO	45	75.00
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Se requiere de grupos de alumnos para encomendar materiales y tareas en actividades del proceso de aprendizaje utilizando recursos tecnológicos?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 34 se reconoce que el 75.00% de los docentes, personal administrativo y alumnos encuestados refirieron que NO se requiere de grupos de alumnos para encomendar materiales y tareas en actividades del proceso de aprendizaje utilizando recursos tecnológicos, mientras que el 25.00% indica que SI lo requiere.

Tabla Nro. 35: Intercambio de Conocimientos

Distribución de frecuencias y respuestas relacionadas al intercambio de reflexiones, experiencias y productos que coadyuven a la actividad del docente y alumno a través de las tecnologías, para la Propuesta de Implementación Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	**n**	**%**
SI	17	28.30
NO	43	71.70
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los docentes, personal administrativo y alumnos encuestados respecto a la pregunta: ¿Se utilizan las TIC para la comunidad educativa en general con miras a intercambiar reflexiones, experiencias y productos que coadyuven a la actividad del docente y alumno?, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 35 se analiza que el 71.70% de los docentes, personal administrativo y alumnos encuestados expresan que NO se utilizan las tecnologías para la comunidad educativa en general con miras a intercambiar reflexiones, experiencias y productos que coadyuven a la actividad del docente y estudiante, mientras que el 28.30% indica que SI las usan.

A. Dimensión 01: NIVEL DE SATISFACCIÓN CON RESPECTO A LA SEGURIDAD INFORMÁTICA EN LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Tabla Nro. 36: Dimensión nivel de satisfacción de la seguridad informática en las Tecnologías de Información y Comunicación

Distribución de frecuencias y respuestas relacionadas con la dimensión 01: Nivel de Satisfacción con respecto a la Seguridad Informática de las TIC, para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	n	%
SI	15	25.00
NO	45	75.00
TOTAL	60	100.00

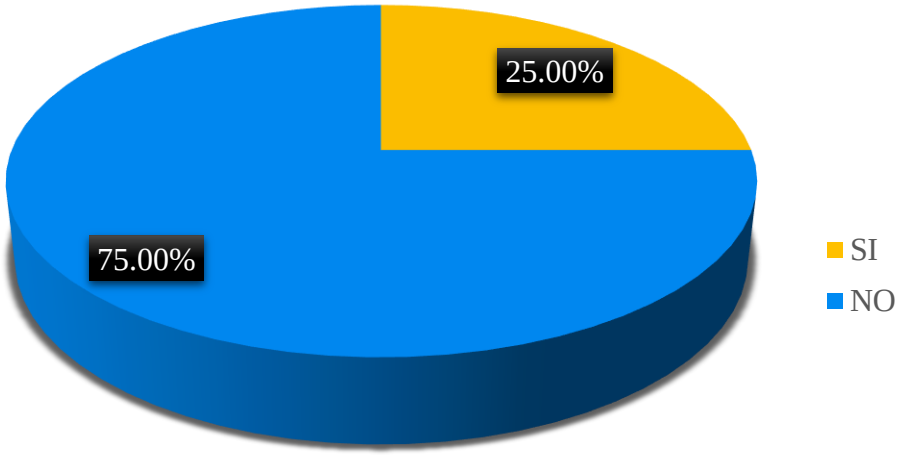
Fuente: Aplicación del instrumento para medir el nivel de satisfacción respecto a la Seguridad Informática en las TIC, basada en 10 preguntas aplicadas a los docentes, personal administrativo y alumnos para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 36 se puede interpretar que el 75.00% de los docentes, personal administrativo y alumnos encuestados NO están satisfechos con la seguridad informática en las TIC, mientras que el 25.00% SI están satisfechos.

Gráfico Nro. 06: Resultados de la Dimensión nivel de satisfacción de la seguridad informática en las Tecnologías de Información y Comunicación.

.



Fuente: Tabla Nro. 36

B. Dimensión 02: NIVEL DE SATISFACCIÓN CON RESPECTO A LA FORMACIÓN Y CAPACITACIÓN A LOS DOCENTES, PERSONAL ADMINISTRATIVO Y ALUMNOS SOBRE EL MANEJO DE LAS TIC

Tabla Nro. 37: Dimensión nivel de satisfacción de la formación y capacitación a los docentes, personal administrativo y alumnos sobre el manejo de las TIC

Distribución de frecuencias y respuestas relacionadas con la dimensión 02: Nivel de Satisfacción con respecto a la formación y capacitación a los docentes, personal administrativo y alumnos sobre el manejo de las TIC: para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Alternativa	n	%
SI	16	27.00
NO	44	73.00
TOTAL	60	100.00

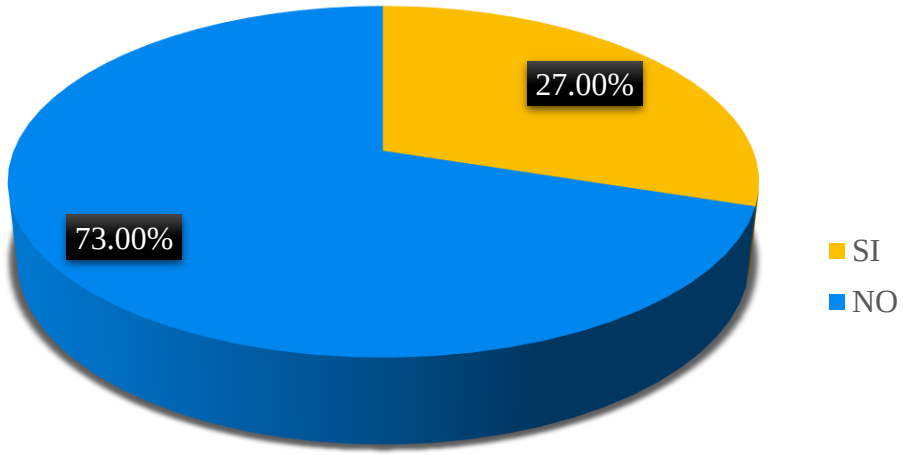
Fuente: Aplicación del instrumento para medir el nivel de satisfacción respecto a la formación y capacitación a los docentes, personal administrativo y alumnos sobre el manejo de las TIC, basada en 10 preguntas aplicadas a los docentes, personal administrativo y alumnos para la Propuesta de Implementación Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 37 se puede interpretar que el 73.00% de los docentes, personal administrativo y alumnos encuestados NO se encuentran satisfechos respecto a la formación y capacitación sobre el manejo de las TIC, mientras que el 27.00% SI están satisfechos.

Gráfico Nro. 07: Resultados de la Dimensión nivel de satisfacción de la formación y capacitación a los docentes, personal administrativo y alumnos sobre el manejo de las TIC

.



Fuente: Tabla Nro. 37

C. Dimensión 03: NIVEL DE SATISFACCIÓN CON RESPECTO A LAS TIC EN EL PROCESO DE ENSEÑANZA APRENDIZAJE

Tabla Nro. 38: Dimensión nivel de satisfacción de las TIC en el proceso de enseñanza aprendizaje

Distribución de frecuencias y respuestas relacionadas con la dimensión 02: Nivel de Satisfacción con respecto las TIC en el proceso de enseñanza aprendizaje: para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

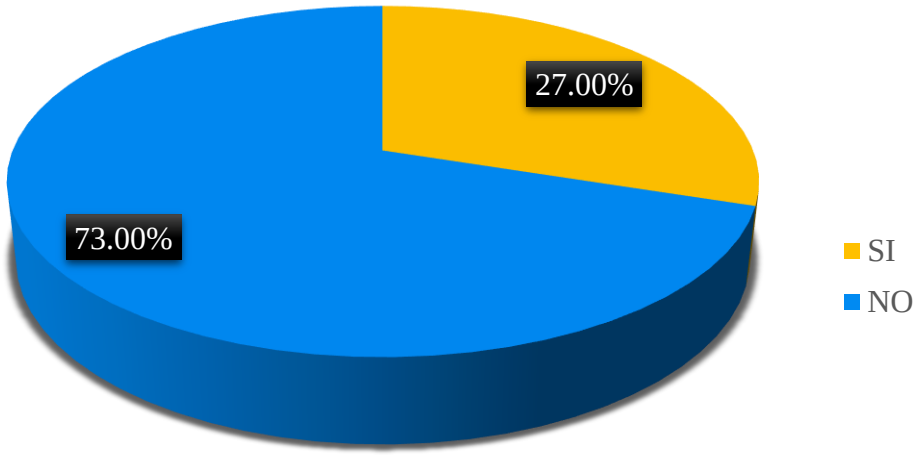
Alternativa	n	%
SI	16	27.00
NO	44	73.00
TOTAL	60	100.00

Fuente: Aplicación del instrumento para medir el nivel de satisfacción respecto a las TIC en el proceso de enseñanza aprendizaje, basada en 10 preguntas aplicadas a los docentes, personal administrativo y alumnos para la Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 38 se puede interpretar que el 73.00% de los docentes, personal administrativo y alumnos encuestados NO se encuentran satisfechos respecto a respecto a las TIC en el proceso de enseñanza aprendizaje, mientras que el 27.00% SI lo están.

Gráfico Nro. 08: Resultados de la Dimensión nivel de satisfacción de respecto a las TIC en el proceso de enseñanza aprendizaje.



Fuente: Tabla Nro. 38

Tabla Nro. 39: Resumen general de Dimensiones

Distribución de frecuencias y respuestas relacionadas con las tres dimensiones definidas para determinar los niveles de satisfacción de los docentes, personal administrativo; para la Propuesta de Implementación de las Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

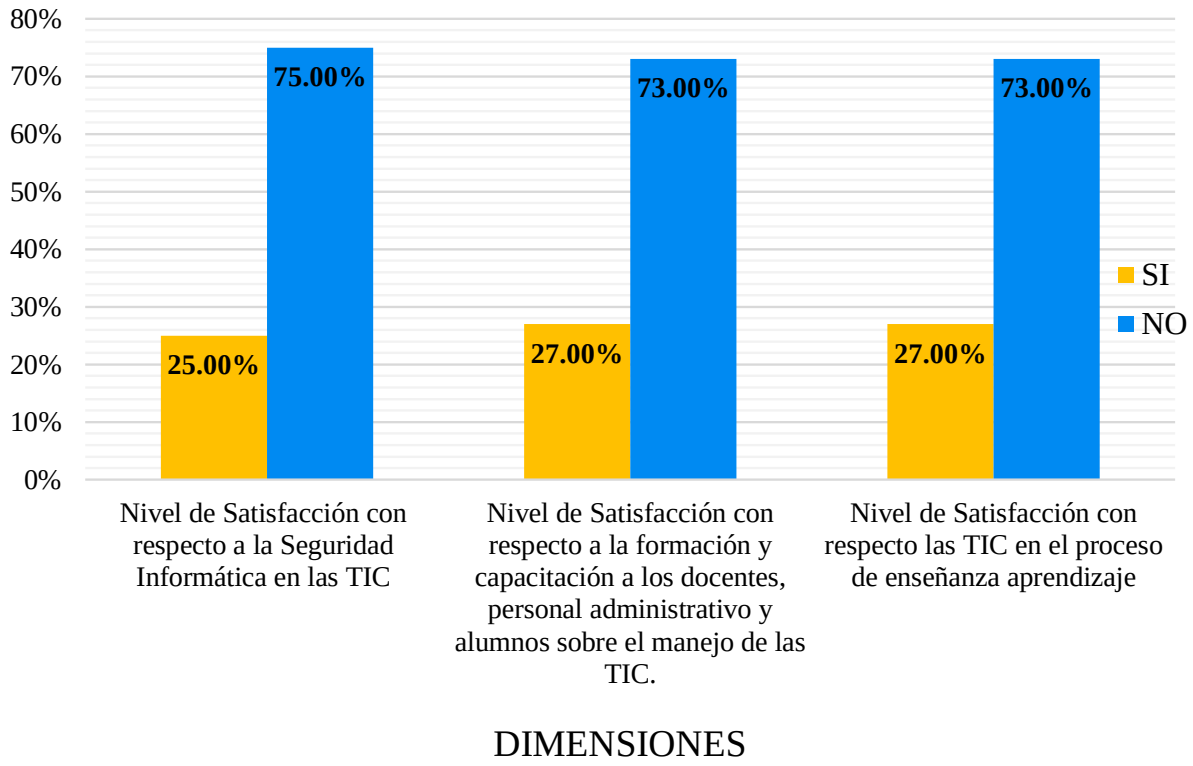
DIMENSIONES	SI		NO		TOTAL	
	n	%	n	%	n	%
Nivel de Satisfacción con respecto a la Seguridad Informática en las TIC.	15	25.00	45	75.00	60	100.00
Nivel de Satisfacción con respecto a la formación y capacitación a los docentes, personal administrativo y alumnos sobre el manejo de las TIC.	16	27.00	44	73.00	60	100.00
Nivel de Satisfacción con respecto las TIC en el proceso de enseñanza aprendizaje	16	27.00	44	73.00	60	100.00

Fuente: aplicación del instrumento para el conocimiento de los docentes, personal administrativo y alumnos acerca de la satisfacción de las tres dimensiones definidas para la investigación: en la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Aplicado por: Aplicado por: Ancajima, M.; 2016.

En la Tabla Nro. 39 se puede observar que en las tres dimensiones el mayor porcentaje de los docentes, personal administrativo y alumnos encuestados expresan que SI están satisfechos con todas ellas, mientras que un menor porcentaje indica que NO.

Gráfico Nro. 09: Resumen general de las dimensiones



Fuente: Tabla Nro. 39

5.2. Análisis de resultados

La presente investigación tuvo como objetivo general: Proponer la implementación de Seguridad informática en las TIC de la I.E. San Miguel Arcángel, la cual mejorará la seguridad informática de la institución y se tendrá un mejor manejo de las TIC; en este aspecto para poder cumplir con este objetivo fue necesario realizar una evaluación de la situación actual con la finalidad de que esta propuesta identifique claramente los requisitos y pueda cubrir las exigencias de la institución a través de una propuesta de mejora seria y técnica.

Para llevar a cabo esta sección de análisis de resultados se diseñó un cuestionario estructurado en 03 dimensiones, los cuales luego fueron aplicados a los docentes, personal administrativo y alumnos de la institución educativa, a través de los procedimientos de recolección de datos. Podemos precisar que los resultados obtenidos e interpretados en la sección anterior, se procede a realizar el siguiente análisis:

1. En lo que respecta a la dimensión 01: Nivel de Satisfacción con respecto a la se Seguridad Informática en las TIC, la Tabla Nro. 36 nos muestra los resultados donde se puede apreciar que el 75.00% de los docentes, personal administrativo y alumnos encuestado expresó que SI considera que la seguridad informática en la institución no es buena, por lo que este producto es similar al resultado que ha obtenido Maza (41), en su investigación donde obtuvo que el 80.00% NO se encontraban satisfechos con la seguridad en la empresa; de la misma forma coincide con los resultados obtenidos por Villasmil (42), la cual da como resultado que el 80.00% NO se encuentra satisfecho, para una dimensión similar a la presente. Esta similitud en los resultados se justifica porque en las instituciones analizadas se evidencia que no existe

mucha seguridad informática mediante las TIC por lo que esto ocasiona, insatisfacción.

2. Asimismo en lo relacionado a la dimensión 02: Nivel de Satisfacción con respecto a la formación y capacitación a los docentes, personal administrativo y alumnos sobre el manejo de las TIC, la Tabla Nro. 37 nos muestra los resultados donde se puede apreciar que el 73.00% de los docentes, personal administrativo y alumnos encuestado expresó que NO se encuentran satisfechos con que la institución les brinda la formación y capacitación sobre el manejo de las TIC, por lo que este resultado es similar al resultado que ha obtenido Alva (43), en su investigación donde obtuvo que el 70.80% NO se encontraban satisfechos, para una dimensión similar a la presente. Esta similitud en los resultados se justifica porque en la institución no les brinda las capacitaciones que corresponde para el manejo adecuado de las TIC por lo que esto ocasiona, insatisfacción.

3. En lo que respecta a la dimensión 03: Nivel de Satisfacción con respecto a las TIC en el proceso de enseñanza aprendizaje, la Tabla Nro. 38 nos muestra los resultados donde se puede apreciar que el 73.00% de los docentes, personal administrativo y alumnos encuestado expresó que NO se encuentran satisfechos con el uso de las TIC en el proceso de enseñanza, por lo que este producto es similar al resultado que ha obtenido Prado (44), en su investigación donde obtuvo que el 95.00% NO se encontraban satisfechos, para una dimensión similar a la presente. Esta similitud en los resultados se justifica porque en las instituciones analizadas se evidencia que el uso de las TIC ayuda en la enseñanza y a la vez ayuda en la seguridad informática mediante ellas por lo que esto ocasiona, satisfacción.

5.3. Propuesta de mejora

Después de haber analizado cada uno de los resultados de la presente investigación, aplicando los instrumentos necesarios y haber realizado la observación correspondiente, se vio la necesidad de realizar la presente propuesta la cual tiene como objetivo ayudar en la mejora continua en los procesos que se desarrollan en la institución, ya que puede servir como punto de inicio para los proyectos tecnológicos que estos tengan en cuenta, empezando con ello a eliminar las bases de información y equipos obsoletos, aumentando la eficiencia y distribuyendo información entre todo el personal de la institución (docentes, alumnos y personal administrativo), minimizando el tiempo y mejorando la calidad de enseñanza; por lo cual se sugiere las siguientes propuestas de mejora:

1. Se sugiere para mejorar la implementación de la Seguridad Informática en la I.E. San Miguel Arcángel, que se realice una reunión con los encargados del área de informática, para que mediante el proceso de administración se pueda generar un mejor control y poder así definir nuevas políticas de seguridad, incluyendo un monitoreo en cuanto a las personas que tienen el acceso a los laboratorios y así mismo realizar pruebas de manera periódica para así evitar cualquier tipo de riesgo y se puedan realizar las acciones correctivas efectivamente ante cualquier incidente que se presente. Para crear nuevas políticas para la seguridad de información de la institución se debe de tener en cuenta la norma ISO 27001 ya que este es un estándar de calidad general.

2. De acuerdo a la investigación que se realizó se propone realizar un manual con todas las políticas de seguridad establecidas con información relevante, clara y concisa donde los docentes, alumnos y personal administrativo puedan mantenerse informados, y así poderlos cumplir para no generar ni un tipo de perdida. Teniendo como base los resultados

obtenidos se estableció el siguiente manual para la I.E. San Miguel Arcángel:

Manual de Políticas de Seguridad para la I.E. San Miguel Arcángel

1. ISO 27001

Para proceder a realizar nuevas políticas de seguridad para la I.E lo que se debe de tener en cuenta es lo siguiente:

a) La política tiene que adaptarse a la institución, es decir que no puede copiar cualquier política que se le cruce, mucho menos si es de una organización mayor.

b) Es necesario definir un marco donde se pueda realizar una investigación a fondo para así poder establecer todos los objetivos de seguridad de la información.

c) La política tiene que presentar el compromiso de dirección para cumplir con los requisitos que presentaran mediante un documento las partes interesadas para así poder mejorar de forma continua el Sistema de Gestión de Seguridad de la Información.

d) Se debe de dar a conocer las nuevas políticas a toda la institución y a todas las partes interesadas, es mejor si se da una capacitación de estas, caso contrario designar un

responsable que se encargue de infórmalas de manera continua.

e) La política debe ser revisada de forma continua, dirección deberá de designar a un responsable para mantenerlas actualizadas y estas continúen vigentes.

2. Políticas de Seguridad Física

a) Acceso Físico

- Los equipos tecnológicos deberán de estar debidamente protegidos bajo la infraestructura apropiada dentro de la institución, de manera que cualquier persona no tenga acceso físico directo.

- Para el acceso a terceras personas estas deberán de ser identificadas, y llevar un control de quienes ingresan y salen a una determinada hora.

- Al momento de ingresar este debe de contar con una identificación que le brinde dirección o personal encargado de los equipos tecnológicos. Al ceder el acceso a los laboratorios estos deberán de ser acompañados por una persona encargada, la cual pueda ayudarlos en lo que este desee manejar.

- El personal encargado para mover, cambiar o retirar algún equipo tecnológico, debe de llenar un formato llenando datos del equipo y la acción a realizar para luego entregarlo a dirección, dándole así la autorización.

b) Protección Física

- En la infraestructura se debe de tener en cuenta los estándares vigentes de cableado estructurado al diseñarse nuevos laboratorios, en la actualización o expansión de estos.

- Se debe de tener un plano de todas las instalaciones eléctricas y de las instalaciones de red de los equipos tecnológicos.

- No se debe de permitir instalaciones improvisadas ni sobrecargadas.

- Para realizar instalaciones estas deberán de ser supervisadas y controladas mediante las pautas que se den.

- Los equipos deberán de ser limpiados una vez por semana, ya que este debe de estar alejado del contacto con el polvo.

- Contar con extintores especiales cerca de donde se encuentran los equipos tecnológicos.

c) Control

- Para el mejor manejo de los recursos tecnológicos y licenciamiento de software se debe de llevar un control total y sistematizado.

d) Respaldos

- Las Bases de Datos de la Institución deberán de tener copias de seguridad y estas ser actualizadas constantemente.

- La Base de Datos principal debe de tener una copia de respaldo alojada en un lugar seguro (Cloud), al igual que una copia general, distante a los equipos de trabajo.

- Se debe generar un correo en Gmail el cual nos da opciones como Google Drive para guardar nuestras copias de respaldo.

- Para tener más seguridad de la información de las personas involucradas (docentes, alumnos y personal administrativo) cada uno deberá generar una copia de respaldo de su información y guardarlas en dispositivos de almacenamiento o discos duros que ellos utilicen, o caso contrario cada uno deberá de contar con un correo y subir a la nube (Google Drive) su información y realizar una constante sincronización de esta. Haciendo a cada una de las personas involucradas (docentes, alumnos y personal administrativo) responsables de sus respaldos de su información.

- Las personas que ingresen a los laboratorios no pueden quitar ni mover ningún tipo de información que se encuentre en ellas, a menos que sea una persona encargada de mantenimiento o personal encargado, y la información sea de carácter ilegal y esta ponga en peligro el funcionamiento de los sistemas, o caso contrario sea virus el que ha infectado la computadora.

e) Recursos tecnológicos de las personas involucradas (docentes, alumnos y personal administrativo)

- Los docentes, personal administrativo y alumnos deberán de cuidar, respetar y realizar un buen uso de los recursos tecnológicos y de la red de la institución siguiendo cada una de las políticas que están en este documento.

- Los docentes, personal administrativo y alumnos deberán de pedir ayuda ante cualquier duda que tenga, al personal encargado de los equipos tecnológicos.

- El correo electrónico debe de tener un buen manejo por parte de docentes, personal administrativo y alumnos, ya que solo es para manejo de la institución y no para envíos de otra índole.

- Está prohibido revisar, realizar copias y almacenar programas, software y demás documentos que violen la ley de derechos de autor, si es de realizar una de estas acciones se debe de firmar un documento comprometiéndose a darle un buen uso, todo bajo firma de dirección y revisión del encargado de los equipos tecnológicos.

- No se debe instalar cualquier programa en los equipos tecnológicos sin dicha autorización por parte de dirección o bajo supervisión del encargado de los equipos tecnológicos.

- No está autorizada la descarga de internet.

- En caso de que cualquier persona realice copias no autorizadas de programas y/o software que no esté permitido, así como cualquier tipo de descargas estas no serán toleradas, y serán llevados a dirección.

- Si una de las personas involucradas (docentes, alumnos y personal administrativo) (docente, personal administrativo y alumnos) es descubierta copiando documentos, información, programas y software para dárselas a terceras personas, serán sancionados, suspendidos o expulsados de la institución, por lo mismo que en caso de copias ilegales de programas informáticos,

según leyes de derecho de autor quedaran sujetas a sanciones civiles y penales, si es grave el caso estas serán mutadas y llevadas a prisión.

- Si se entera u observa cualquier uso inadecuado haya con los equipos tecnologías en la institución deberá informar al encargado de los equipos tecnológicos y/o dirección.

3. Políticas de Seguridad Lógica de la Red

a) Red

Las redes tienen como objetivo principal el intercambio de información dentro de la institución, por lo que se deberán de cumplir las siguientes políticas:

- El área tecnológica no es responsable del contenido de la información ni tráfico que haya en ello, la responsabilidad es directamente de la persona que lo genere.

- No se puede ver, copiar, modificar o eliminar la información que radica en los equipos sin el consentimiento del administrador del equipo.

- Las cuentas de acceso a los sistemas y los recursos tecnológicos son propiedad de la institución y serán utilizados exclusivamente para las actividades que se desempeñen.

- Las cuentas de acceso a los sistemas y recursos tecnológicos son personales e intransferibles, su uso es único durante la vigencia de derechos de autor.

b) Servidores

- Los encargados de mantenimiento tienen la responsabilidad de verificar, la instalación, configuración e implementación de seguridad, en los servidores conectados a la red.

- Toda instalación y/o configuración que se realice en la red queda bajo responsabilidad de los encargados de mantenimiento.

- Cuando se desarrolle la configuración de los servidores los encargados de mantenimiento deberán de realizar normas para el uso de recursos del sistema y de la red, restringiendo los directorios, permisos y programas que serán ejecutados.

- Los servidores que proporcionen servicios a través de la red e internet deberán:

    1. Funcionar las 24 horas del día los 35 días al año.

    2. Dar un buen mantenimiento preventivo mínimo dos veces al año.

    3. Dar mantenimiento anual a la revisión de la configuración.

- Se debe realizar copias de respaldo de la información de los servidores como mínimo:

    1. Diariamente si la información es crítica.

    2. Semanalmente a los documentos web.

    3. Mensualmente a la configuración del servidor y logs.

- El servicio de internet solo se dará mediante los servidores autorizados.

- Cada usuario debe de contar con su cuenta de correo electrónico en el uso de los servidores que administra, en caso de dirección y administración de la institución.

- Para efecto de asignarle su cuenta de correo al usuario, este deberá llenar una solicitud de formato libre y entregarlo al área de informática.

- La cuenta debe de llevar su nombre y apellidos para poder ser identificados.

- Los servidores deberán de estar ubicados en un área física que cumpla con las normas para un centro tecnológico:

    1. Acceso restringido

    2. Temperatura adecuada para el equipo

    3. Protección contra descargas eléctricas

    4. Mobiliario adecuado que garantice la seguridad de los equipos

- El administrador de la base de Datos no debe de eliminar ni un tipo de información del sistema, excepto si la información este obsoleta o ponga en riesgo el funcionamiento del sistema.

c) Recursos tecnológicos

- El personal de mantenimiento será el encargado de suministrar medidas de seguridad adecuadas contra la intrusión o daños de la información almacenada en los sistemas así como en la instalación de cualquier dispositivo o software que refuerce la seguridad en los equipos de tecnológicos.

- En la seguridad de hardware se debe hacer uso de dispositivos como contrafuegos o firewalls de hardware y servidores proxy. Se debe de realizar un análisis de qué tipo de seguridad deberán de tener los equipos ya que lo primero en evaluar son las vulnerabilidades en las que se encuentra.

- En la seguridad de software se debe mantener actualizados los antivirus, al momento de que una de las personas involucradas (docentes, alumnos y personal administrativo) conecte un dispositivo de almacenamiento este pueda ser analizado con tal de evitar ataques maliciosos que dañen información que contenga la institución.

- El personal de mantenimiento debe de tener informados a las personas involucradas (docentes, alumnos y personal administrativo) sobre el software que refuerce la seguridad de los equipos y ponerlos a su disposición.

- El personal de mantenimiento debe de ser el único autorizado en monitorear el tráfico de paquetes en la red, con el fin de detectar dar solución a situaciones que se presenten, al igual que registrar usos indebidos o detectar fallas que provoquen los problemas de servicio en la red.

- El personal de mantenimiento deberá ingresar a la computadora de dirección y administración exclusivamente para dar solución a los problemas que esta tenga siempre y cuando tenga los permisos del propietario.

- El personal de mantenimiento debe de tener actualizada la información de los recursos de los equipos que este tenga a cargo, esto siempre y cuando se adquiera o se instale nuevos equipos o software.

- Se debe tener un inventario utilizando programas de Microsoft, en el cual se tendrán todos los datos actualizados de los equipos tecnológicos que se encuentren en la institución.

- Las computadoras deberán de ser revisadas periódicamente para verificar que haya existencia de archivos no autorizados, música, configuraciones no validas o permisos extras que pongan en riesgo la seguridad de la información.

- Se debe realizar los reportes a dirección en cuanto a incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas tecnológicos.

- Para los equipos tecnológicos se debe de estimar un tiempo de vida útil para así tener programado una anticipación de renovación.

- En caso de que un equipo tecnológico presente problemas, de arranque u otros reportar al personal de mantenimiento y este deberá presentar un documento a dirección reportando el daño del equipo.

d) Uso de servicios de red

- La dirección debe de definir los servicios de internet que va a ofrecer en la institución os cuales deberán de ser coordinados con el personal de mantenimiento para proceder a la configuración correspondiente.

- Los encargados de mantenimiento son responsables de la administración de cada una de las contraseñas y desean guardar su confidencialidad.

- No se brindara ni un equipo, ni contraseñas, ni cuentas de correo a personas que presten servicio social o personas que realicen sus prácticas profesionales dentro de la institución, en caso se requiere de alguna, estas deberán llenar un documento solicitando el servicio que desee a dirección.

- Los encarados de mantenimiento deberán de realizar las siguientes actividades en los servidores:

1. Respaldo de la información siguiendo los procedimientos establecidos.

2. Revisión de logs y realizar reportes de cualquier eventualidad que se dé.

3. Implementar de manera inmediata las recomendaciones de seguridad y reportar las faltas que se den a las políticas de seguridad.

4. Tener un monitoreo de los servidores que tengan asignados.

5. Organizar y supervisar al personal encargado de mantenimiento.

- Los encargados de mantenimiento deberán aislar cualquier servidor de red, notificando a la dirección, en caso que se den las siguientes condiciones:

    1. Si es que en los servidores se implica un tráfico adicional que impida el buen funcionamiento de la red.

    2. Si se detecta vulnerabilidades que comprometan la seguridad de la red.

    3. Si se detecta programas que alteren la legalidad y consistencia de los servidores.

    4. Si se detectan accesos no autorizados comprometiendo la integridad de la información.

    5. Si son violadas las políticas de uso de los servidores.

    6. Si se reporta un tráfico adicional que dale la red de la institución.

- Los docentes y personal administrativo que tengan el acceso a uno del sistema de información o la red, deberán tener la autorización de un usuario y contraseña.

- Cada una de las personas involucradas deberá recibir información de las políticas de seguridad informática y aplicarlas en la institución.

- Los docentes y personal administrativo tendrá acceso exclusivamente a aquellos datos y recursos que solo sea útil para la función de sus actividades, siguiendo las políticas establecidas.

- Las contraseñas deberán tener como máximo 8 caracteres combinando números, letras y caracteres especiales.

- Las personas que cuenten con un usuario y contraseña, deberán de tener en cuenta que la contraseña debe de ser actualizada constantemente y colaborar con los encargados de mantenimiento con el fin de contribuir a la seguridad de los servidores.

- Las personas que cuenten con un usuario y contraseña deberán informar si observan cualquier comportamiento anormal como mensajes extraños, correos spam o lentitud en la red o algún problema inusual dentro del servidor o caso contrario tenga problemas al acceder a los servicios que este brinda.

- Las personas que tengan un usuario y contraseña tienen la responsabilidad de utilizar su acceso para realizar cualquier eventualidad que esta requiera.

- Está prohibido la revelación del usuario y contraseña a terceras personas, cada uno es responsable de sus identificadores, por lo tanto evitar escribirlos en lugares visibles para otras personas.

- Los docentes y personal administrativo no debe de ingresar a cuentas que no estén autorizadas.

- Si un docente o personal administrativo sospecha que han accedido a su cuenta sin autorización, cambie inmediatamente su contraseña y recurra al personal de mantenimiento para reportar de inmediato al responsable.

- Deberán realizar una copia de seguridad a toda la información que se tenga.

- Los datos más importantes deberán ser cargados a dispositivos de almacenamiento, protegiéndolo ante revelaciones, modificaciones, destrucción o mal uso.

- Guardar sus dispositivos de almacenamiento en un lugar seguro donde solo usted los pueda visualizar, evitando a terceras personas.

- Las personas involucradas solo podrán crear ficheros temporales que contengan datos de aspecto personal para un uso personal, siempre y cuando sea utilizado en el desempeño de sus actividades. Después de utilizar los ficheros estos deberán de ser guardados en un dispositivo de almacenamiento externo, para luego ser borrados del equipo.

- Los recursos informáticos como Datos, software, red y sistemas solo estarán disponibles para el uso exclusivamente de actividades dentro de la institución.

- Queda prohibido el uso de los recursos tecnológicos para actividades relacionadas a negocios o para la realización de descargas de música y video.

- Queda prohibido utilizar los equipos de trabajo para ocasionar daño como amenazas, contenidos obscenos inmoralidades o cosas ofensivas a terceras personas.

- Está prohibido destruir, alterar, inutilizar o realizar cualquier tipo de daño a los datos de programas o documentos que se encuentren en los equipos de trabajo.

- Queda prohibido guardar datos de carácter personal en las unidades locales de los equipos de trabajo.

- Queda prohibido los ficheros que sean introducidos en la red o en el equipo de trabajo a través de soportes automatizados, internet, correo electrónico o cualquier medio, estos deberán de cumplir con los requisitos establecidos en estas políticas, teniendo en cuenta las referidas a propiedad intelectual y control de virus.

e) Antivirus

- Todos los equipos de trabajo de la institución deberán de tener instalada una solución de Antivirus.

- Periódicamente se debe se hace el rastreo en los equipos de trabajo y deberá de realizarse la actualización de firmas del antivirus proporcionada por el fabricante.

- Los encargados de mantenimiento son responsables que en cada equipo, trabaje correctamente el antivirus.

- Configurar el analizador correctamente para la detención de virus.

- Al ser detectado un virus, los encargados de manteamiento deberán de actuar rápidamente.

- Cada vez que se haga uso de USB, discos estos deberán de ser analizados por el antivirus del equipo de trabajo.

- Los encargados de mantenimiento deberán de aislar el equipo, notificando a dirección las condiciones en la que se encuentra como:

1. Cuando el virus no puede ser controlado, con el fin de que se evite la propagación del virus a otros equipos.

2. En caso que las personas involucradas violen las políticas del antivirus.

f) Operación en los laboratorios de cómputo

- La dirección podrá ofrecer servicios de computación, soporte técnico y servicios audiovisuales para el dictado en clases en los laboratorios que están disponibles

- La dirección deberá dar a conocer dichas políticas a cada uno de sus integrantes en la institución mediante charlas introductorias y copias del documento.

- La administración de los servicios de la red deben de llevarse a través de métodos automatizados.

- Los encargados de mantenimiento deben de verificar el nivel de seguridad en que se encuentra el software que se ha instalado en los equipos de trabajo.

- Se podrá asesorar a las personas que necesiten ayuda en el manejo de las TIC.

- La institución deberá contar con personal de mantenimiento para cualquier eventualidad que se desarrolle con los recursos tecnológicos.

- Equipo de cómputo, la persona que lo esté utilizando deberá de reportarla para que esta sea reparada o lograr notificarlo para que tome las medidas correspondientes.

g) General

- Cualquier acción que esté en contra de las políticas de seguridad en los equipos tecnológicos debe de ser sancionadas con la suspensión por un periodo determinado bajo el conocimiento de dirección.

NOTA: Para crear una política no es necesariamente realizar un documento extenso con todas las reglas de seguridad de información que existan, simplemente dentro del documento deben de estar detalladas las políticas que se adaptan a la institución entre ellas políticas de control de acceso, política de clasificación, política de utilización aceptable, etc.

3. Una de estas propuestas más importantes es capacitar a los docentes, alumnos y personal administrativo a través de talleres informáticos en cuanto al uso correcto de las TIC, brindarles información adecuada y explicándoles detalladamente que es lo que se puede realizar con estas herramientas tecnológicas tomadas de la mano con procedimientos planteados y las políticas de seguridad establecidas, así como ayudarlos a que los docentes y alumnos tengan una mejor interacción con las TIC; donde los docentes puedan hacer el dictado de sus clases con las herramientas tecnológicas que les ofrece el estado, haciendo sus temas más interesantes donde el alumno pueda poner atención; igual para el alumno al conocer sobre el adecuado manejo de las TIC podrá elevar sus conocimientos y poder desarrollar grandes cosas.

4. Finalmente, proponiendo que las políticas establecidas y las capacitaciones que se brinden a toda la población institucional sea manejada bajo un control y sean gestionados, para que así se genere una supervisión constante y directa de las actividades o procesos que se van a realizar, ya que ayuda a resguardar la integridad de datos, así como el avance efectivo de trabajo,

minimizando costos de riesgo. No olvidar que como norma predeterminada es importante respaldar su información.

Gráfico Nro. 10: Fotografía laboratorio de Cómputo (1)

Fuente: Fotografía propia

Gráfico Nro. 11: Laboratorio de Cómputo (2)

Fuente: Fotografía propia

Gráfico Nro. 12: Laboratorio con Seguridad

Fuente: Elaboración Propia

VI. CONCLUSIONES

Correspondiente a los resultados obtenidos en el trabajo de investigación, se puede concluir que en la I.E. San Miguel Arcángel es necesaria la implementación de la Seguridad Informática en las TIC, este resultado coincide con lo planteado en la hipótesis general, por lo que se deduce, a que dicha hipótesis queda aceptada.

Según los resultados se puede concluir lo siguiente:

1. El 75.00% de los docentes, alumnos y personal administrativos indican que no se están satisfechos con la Seguridad Informática dentro de la I.E., por lo que con la investigación detallada llegamos a concluir que las TIC que se encuentran en dicha organización no tienen el manejo adecuado para resguardar su información ya que bien puede ser robada, plagiada, o ser alterada para fines maliciosos, que perjudicarían y preocuparían a la institución.

2. Un 73.00% de las personas en general encuestadas en la I.E. San Miguel Arcángel se ha dado como resultado que no se encuentran satisfechos respecto a la formación y capacitación del manejo de las TIC en lo que concierne en la seguridad informática ya que ellos lo ven muy necesario para el desarrollo a nivel educativo, favoreciendo nuevos conocimientos que ayudan a mejorar las capacidades de todo personal de la institución.

3. El 73.00% de las personas encuestadas arrojo como resultado una insatisfacción de las TIC en el proceso de enseñanza aprendizaje, por lo que llegamos a la conclusión de que a pesar que la institución cuenta con herramientas TIC adecuadas, no tienen la iniciativa de generar una buena implementación de enseñanza entre el docente y alumno, así como también podemos afirmar que al momento de que el docente y personal administrativo utilice un software, cualquier usuario pueda ingresar y

extraer su información, perjudicándolos y generando problemas con las políticas establecidas.

RECOMENDACIONES

1. Se debería desarrollar como iniciativa la práctica de herramientas TIC en la elaboración del dictado de clases, así como también la utilización de estas para mantener la información de la institución segura ante cualquier eventualidad maliciosa.

2. Se sugiere la implementación de políticas de Seguridad Informática; para la cual ayudará a la institución a que se tenga un mejor manejo en las herramientas TIC, de manera adecuada.

3. Es necesario realizar un taller de capacitación para los docentes, alumnos y personal administrativo, el cual tenga como objetivo mostrar el manejo adecuado de las herramientas TIC, así como también el manejo de software para el cuidado de su información y ellos puedan aplicarlo en la actualidad.

REFERENCIAS BIBLIOGRÁFICAS

1. Gómez Vieites Á. Auditoría de seguridad informática España: RA-MA Editorial; 2014.

2. Espiñeira SYA. Seguridad de la Información: Un nuevo enfoque para el control de Riesgos de Negocio. [Online].; 2005 [cited 2016 mayo 3.

3. A.B.C N. Programa avanzado de estudio: seguridad en sistemas de informacion. 2nd ed. Venezuela: CompTIA; 2010.

4. Burgos J CP. Modelo para la Seguridad en TIC. Monografía. Concepción,Chile: Universidad del Bío-Bío, Departamento de Informática; 2008.

5. Ramas Arauz F. TIC en educación: escenarios y experiencias Mexico: Ediciones Díaz de Santos; 2015.

6. Bermúdez Molina KG, Bailón Sánchez ER. Análisis en Seguridad Informática y Seguridad de la Información basado en la Norma ISO/IEC 27001- Sistemas de Gestión de Seguridad de la Información dirigido a una Empresa De Servicios Financieros. Tesis Grado. Guayaquil: Universidad Politécnica Salesiana ; 2015.

7. Paula Reynoso RA, Rosario Frías M. Análisis de la Gestión de la Seguridad de Tecnologías de la Información (TI),en las Pequeñas y Medianas Empresas de San Francisco de Macorís. Tesis Grado. República Dominicana: Universidad Autónoma de Santo Domingo, Departamento informática; 2016.

8. Chicano Tejada E. Gestión de incidentes de seguridad informática. Primera ed. España: IC Editorial; 2014.

9. Arnedo Moreno J. Redes de comunicaciones. Primera ed. Barcelona: Editorial UOC; 2013.

10. González Uní LC. Estrategias para optimizar el uso de las TIC y su seguridad informática en la práctica docente que mejoren el proceso de aprendizaje. Tesis

Magister. Bucaramanga, Santander, Colombia: Universidad Autónoma de Bucaramanga, Departamento Tecnológico; 2012.

11. Martinez Cabrera JB. Implementación de un Sistema de Control de acceso a red en la Empresa Sima. Tesis Grado. Chimbote: Universidad Católica los Angeles de Chimbote, Departamento de Ingeniería; 2018.

12. Villanueva Flores CE. Diseño del sistema de gestión de seguridad de la información para el grupo SIAS SAC. Tesis grado. Chimbote: Universidad Catóñica los Angeles de Chimbote, Departamento de Ingeniería; 2017.

13. Castillo Coolazos RE. Sistema de Gestión de Seguridad de la Información en la Municipalidad Distrital de Pira aplicando la Norma ISO/IEC 27001:2013. Tesis Grado. Huaraz, Peru: Universidad Católica los Angeles de Chimbote, Depaartamento de ingeniería; 2016.

14. Alcántara Flores JC. Guía de Implementación de la Seguridad Basado en la Norma ISO/IEC 27001, para apoyar la Seguridad en las TIC de La Comisaria Del Norte P.N.P en la Ciudad de Chiclayo. Tesis Grado. Chiclayo: Universidad Católica Santo Toribio de Mogrovejo, Departamento de Sistemas y Computación; 2015.

15. Gil Villanueva CJ. Implementación de mecanismos de Seguridad Informática para el mejoramiento, integridad y protección del software del ITP CITEC del norte. Tesis Grado. Chimbote: Universidad Católica los Angeles de Chimbote, Departamento académico de vicerrectorado de investigación; 2015.

16. Agramonte Albán AM. Auditoría del Sistema de Seguridad de información en el Hospital III José Cayetano heredia. Tesis Grado. Castilla, Piura: Universidad Católica los Angeles de Chimbote, Departamento de Ingeniería; 2016.

17. Figueroa Jiménez MA. Servidor Señuelo Informático Honeynet Híbrido y su influencia en la Seguridad Informática Activa Lógica del Centro de Diálisis Piura. Tesis Grado. Piura: Universidad Cesar Vallejo, Departamento de Ingeniería; 2014.

18. Bocanegra Mimbela AP. Perfil del nivel de gestión del dominio adquirir e implementar de las Tecnologías de la Información y Comunicación (TIC), en el personal docente del I.S.T Hermanos Cárcamo. Tesis Grado. Piura: Universidad Católica los Angeles de Chimbote, Departamento de ingeniería; 2016.

19. Zapata Periche C. Perfil del nivel de gestión del dominio planeamiento y organización de las Tecnologías de Información y Comunicación (TIC) en el personal docente de la Institución Educativa Ignacio Sánchez. Tesis Grado. Piura: Universidad Católica lo Angeles de Chimbote, Deprtamento de ingeniería; 2013.

20. Ramos Arca CE. Propuesta de un Plan de Auditoria Informatica para el "Sistema De Informacion En Salud" y el "Aplicativo Para El Registro De Formatos Sis" en los establecimientos de Salud de la unidad ejecutora 400. Tesis Grado. Piura: Universidad Nacional de Piuraa, Departamento ingeniería Informática; 2015.

21. Rojas Neyra FdM. Conoce a tu Institución. Cronograma Festividad. Catacaos: I.E San Miguel Arcangel; 2015.

22. Google. Google Maps. [Online].; 2016.

23. Competitividad Ad. Tecnologías de Información y Comunicación. Informe. Peru:, Departamento de Economía Tecnológica; 2014-2018.

24. Arevalo Liendo M. Las Tecnologías de Información dentro de las estrategias competitivas. Tesis Maestría. Piura: Universidad de Piura, Dirección Estrategica en Tecnologías de Información; 2009.

25. Mendoza I RV. Uso de las TIC en la Educación. Tesis Doctorado. Venezuela: Universidad del Zulia, Departamento de Ciencias; 2005. Report No.: ISSN 1315-4079.

26. Martinez A. Las TICs repuntarán hacia 2015. El Financiero. 2014 Setiembre: p. 5.

27. Echeverría J. Cosmopolitas Domesticos. Primera ed. Barcelona España: Ed. Ancagrama; 1995.

28. Bossio H, Gros C. Seguridad Informática parte de la Cultura del Control. In Conferencia de Seguridad; 2003; Argentina. p. 91.

29. Laundon K, Laundon J. Sistemas de Información. 6th ed. Santa Fe: Ed. Prentice Hall; 2002.

30. ONGEI. Situación de las Tecnologías de Información y Comunicaciones. Informe. Peru: Oficina Nacional de Gobierno Electrónico e Informática, Departamento de Electronica e Informatica; 2004.

31. Aldana A. Seguridad en las TICs. [Online].; 2015 [cited 2016 mayo 4.

32. Andrés A A, Gomez L. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. Tesis. España: AENOR (Asociación Española de Normalización y Certificación); 2012.

33. Farias Elinos M, Mendoza Diaz MC, Gómez Velazco L. Las Políticas de Seguridad como Apoyo a la Falta de Leegislación Informática. Informe. Techno-Legal aspects of Information Society and New, Departamento de Informatica; 2003.

34. Alvarez Basaldúa LD. Seguridad en la Informacion (Auditoria de Sistemas). Tesis Maestral. Mexico, D.F.: Universidad Iberoamericana; 2005.

35. IT Governance Institute. Information Security Governance:Guidance for Boards of Directors and Executive Management. 2nd ed. EE.UU: IT Governance Intitute; 2006.

36. De la Cruz C, Vazquez JC. Elaboración y aplicación de un sistema de gestión de la seguridad de la informacion (SGSI) para la realidad tecnológica de la USAT. Tesis. Chiclayo: Universidad Catolica Santo Toribio de Mogrovejo; 2008.

37. Sampieri R CCLP. Metodología de la Investigación. Guía Didáctica. México,D.F: McGraw-Hill Interamericana; 2003.

38. Ávila Baray. INTRODUCCIÓN A LA METODOLOGÍA DEL LA INVESTIGACIÓN. 1st ed. Mexico: Instituto Tecnológico de Cd. Cuauhtémoc; 1999.

39. Hernández Sampier R. Metodología de la investigación. Editorial.. 2nd ed. Varela F, editor. La Habana: VarelaX; 2004.

40. Arias F. El proyecto de investigación: Introducción a la metodología científica. 5th ed. Caracas - Venezuela: Episteme; 2006.

41. Maza Anton L. Plan de contingencia informatico y seguridad de informacion. Monografia. Piura: Universidad Nacional de Piura, Departamento de Ingerieria Informatica; 2009.

42. Villasmil F. Análisis de los Riesgos de Seguridad Informatica con las TICs para las pequeñas y medianas empresas (PYME's) usando el Estándar ISO-17799. Tesis Tecnologica. Barquisimo: Universidad Centroccidental "Lisandro Alvarado"; 2006.

43. Alva Arce RC. Las Tecnologías de información y comunicación como instrumentos eficaces en la capacitación a maestristas de educación. Lima: Universidad Nacional Mayor de San Marcos; 2011.

44. Prado Álvarez PJ. Actitud de los Docentes de la carrera de Magisterio Primaria y Preprimaria del Instituto Belga Guatemalteco ante la utilización de las Tecnologías de Información y Comunicación dentro del proceso de enseñanza y aprendizaje. Tesis. Guatemala: Universidad Rafael Landívar; 2012.

45. "Actualización del impacto de las Tecnologías de Información y Comunicación en el Perú". Libro. Lima: INEI, Departamento de Estadistica e Informatica; 2002.

46. Union Europea. Manual Balsico para la Gestion Integrada de las Pymes. Informe. Todo Europa: Fundación Esculapio, Departamento de Financiamiento; 2004.

47. Arnold Cathalifaud M, Osorio F. Introducción a los conceptos básicos de la Teoría General de Sistemas. Revista Electrónica de Epistemología de Ciencias Sociales. 2006 Abril; I(3).

48. Bestratén Belloví M, Carboneras Checa A. Integración de sistemas de gestión: prevención de riesgos laborales, calidad y medio ambiente. Informe. España: Ministerio de Tabajo y Asuntos sociales y Instituto de Seguridad e higiene en el trabajo., Departamento de Desarrollo Industrial; 2006.

49. Burgos Salazar J, G.Campos P. Modelo para la Seguridad en TIC. Monografia. concepcion,Chile: Universidad del Bío-Bío, Departamento de Informatica; 2008.

50. Cámara M, Romain G, Parra Erkel R. Proyecto:"Perú:Situación de las Tecologías de Inforación y Comunicación". Informe Nacional. Lima: Presidencia del Consejo de Ministros, Departamento de Informatica; 2010.

51. Camargo M. Sistema de control de riego automático mediante el monitoreo de humedad del suelo vía internet. tesis. Mexico: Universidad Autónoma de Querétaro, Departamento de Ingenieria; 2013.

52. Camarillo Osorio. Documentacion del Sistema integrado de gestion de la calidad y modelo estandar de control interno de la corporacion autonoma regional del quindio. Tesis para optar titulo. Pereira: Universidad Tecnologica de Pereira, Departamento de Gestión de Calidad y Normalización Tecnica; 2008.

53. Castilla Rondan I, Barrientos Lazo M. Elaboración de un plan de Seguridad de Informacion en la Universidad de Huanuco. Monografia. Huanuco: Universidad de Huanuco, Departamento de Ciencia y Desarrollo; 2008.

54. Cientificos L. Modelado Predictivo para la Inteligencia de Negocios: CreateSpace Independent Publishing Platform; 2015.

55. Cisco. Cisco 2007 Annual Security Report". Cisco; 2007.

56. Colinas Ramírez J. Plan de Seguridad para una pequeña empresa. Tesis. Madrid: Universidad Pontificia Comillas, Departamento de Ingenieria; 2008.

57. Competitividad Ad. Tecnologías de Información y Comunicación. informe. peru:, Departamento de Economia tecnologica; 2014-2018.

58. Córdova Rodríguez. Plan de Seguridad Informatica para una Entidad Financiera. Tesis. Lima: Universidad Nacional Mayor de San Marcos , Departamento de Informatica; 2003.

59. Curto Diaz J. Introducción al Business Intelligence: Editorial UOC; 2012.

60. Diaz C, Edwin P. Diseño Hidráulico y Agronómico para un Sistema de Riego Del Sector la Arenita, Distrito Paiján Chicama. Tesis. Paijan: Universidad Privada Antenor Orrego, Departamento de Ingenieria; 2014.

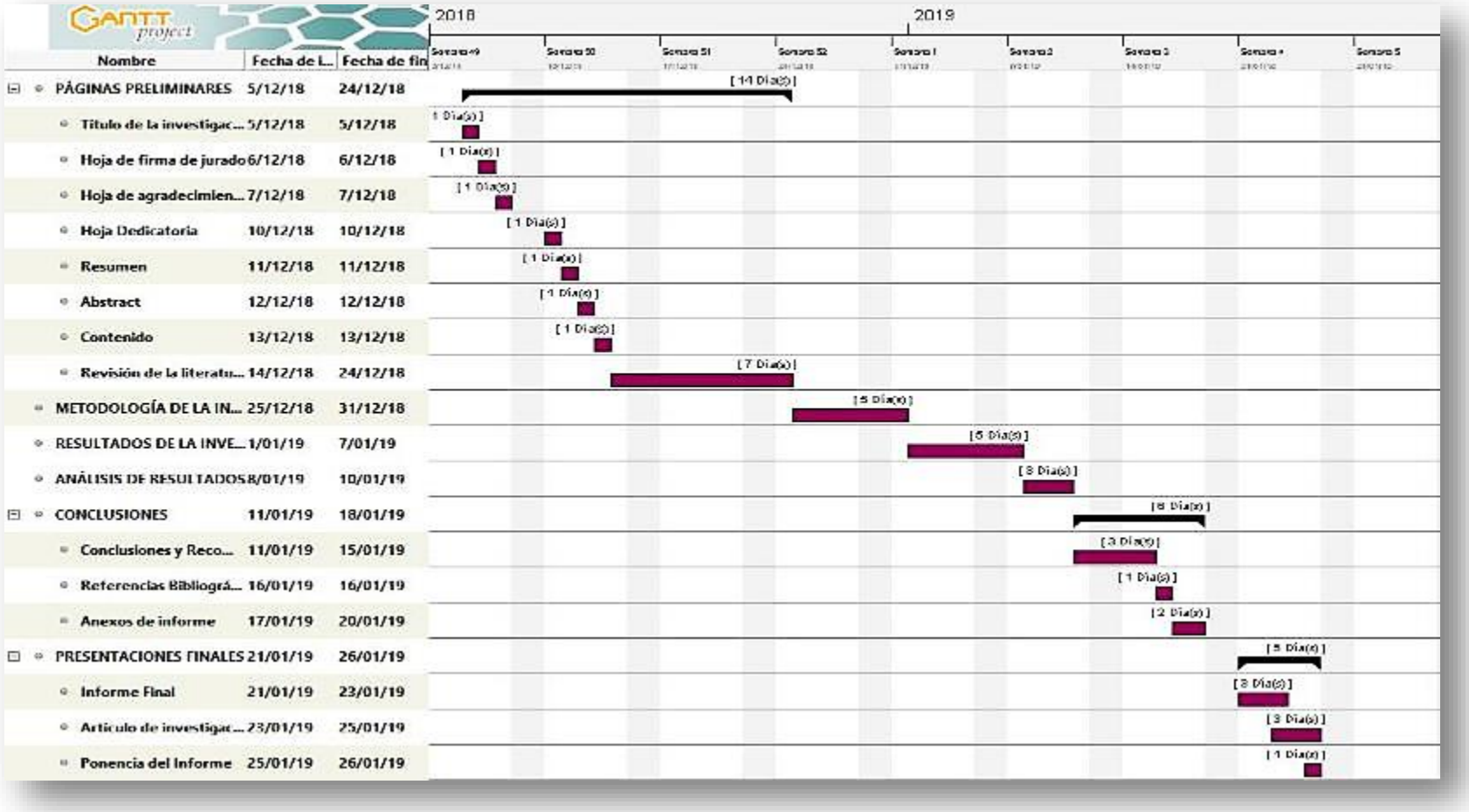
61. E.S. Seguridad de las redes y de la información:Propuesta para un enfoque europeo. Propuesta. Europa: Comunicación de a comisión al consejo, Al Parlamento Europeo, al Comité Económico y Social y al Comité De Las Regiones; 2004.

62. Gómez Vieites Á. Enciclopedia de la Seguridad Informática. 1st ed. Mexico: Alfaomega Grupo Editor; 2007.

63. Marugan Marinero J. "Diseño de infraestructura de Red y Soporte Informático para un centro público infantil y primaria". Tesis. Madrid- España: Universidad Politecnica de Madrid, Departamento de Informatica; 2010.

ANEXOS

Anexo 01: Cronograma de actividades



Fuente: Elaboración Propia

Anexo 02: Presupuesto y financiamiento

Proyecto : Escuela de Ingeniería de Sistemas

Título : "Propuesta de implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016."

RUBRO	CANTIDAD	COSTO UNITARIO (S/.)	COSTO TOTAL (S/.)
MOVILIDAD			
✓ Pasajes Catacaos centro hacia la I.E. y viceversa.	04 pasajes	4.00	16.00
MATERIAL DE ESCRITORIO			
✓ Papelería	½ millar	12.00	12.00
✓ Lapiceros	02 unidades	0.50	1.00
✓ Folder	01 unidad	3.50	3.50
✓ Lápiz	01 unidad	1.00	1.00
✓ Cuaderno	01 unidad	12.00	12.00
✓ USB	01unidad	30.00	30.00
MATERIAL BIBLIOGRÁFICO			
✓ Fotocopias	65 unidades	0.10	6.50
✓ Impresión a tesis y encuesta	107 unidades	0.50	53.50
SERVICIOS			
✓ Internet	12 Meses	50.00	600.00
PERSONAL			
✓ Honorarios Asesorías	28 horas	40.00	1400.00
		TOTAL	2135.50

Fuente: Elaboración Propia

Anexo 03: Instrumentos de recolección de datos

CUESTIONARIO

El presente Cuestionario es parte del trabajo de investigación con el título:

"PROPUESTA DE IMPLEMENTACIÓN DE SEGURIDAD INFORMÁTICA EN LAS TIC DE LA I.E. SAN MIGUEL ARCÁNGEL, CATACAOS - PIURA; 2016."

Por lo que estimados encuestados, dicha investigación necesita de su colaboración, por lo que se le agradece su anticipada participación respondiendo a cada pregunta de manera objetiva y veraz. La información a proporcionar es de carácter confidencial y reservado; y los resultados de la misma serán utilizados solo para la presente investigación.

INSTRUCCIONES:

A continuación se le presentara una seria de preguntas cuya respuesta se debe señalar con una aspa (X), en una escale de valores correspondiente (SI o NO) según considere la alternativa correcta.

Por ejemplo:

Pregunta	SI	NO
1. ¿El Internet en la Institución Educativa es rápido?	X	

DIMENSIÓN Nro. 01		
Encuesta para medir el nivel de satisfacción con respecto a Seguridad informática en las Tecnologías de Información y Comunicación.		
PREGUNTAS	**SI**	**NO**
1. ¿Cree usted que la implementación de seguridad informática en las TIC es la adecuada en su ambiente de trabajo?		
2. ¿Cree usted que la institución considera importante invertir en herramientas TIC?		
3. ¿Considera que el uso de los antivirus en los equipos informáticos de la Institución son seguros cuando ingresa o retira información en algún dispositivo de almacenamiento?		
4. ¿Al navegar por internet, usted cree que existe la seguridad y la confiabilidad necesaria para compartir su información?		
5. ¿La infraestructura de las TIC críticas o con información sensible con la que cuenta la institución, están ubicadas en entornos protegidos y con controles de acceso?		
6. ¿Cree que la seguridad informática de su institución es importante y deben de tomarse las medidas adecuadas de protección?		
7. ¿En su institución educativa existe alguna política de protección de la información que haga que la seguridad sea eficaz, cuando se produce un intercambio electrónico de información?		

8. ¿Usted considera que la institución le brinda la seguridad y protección confiable al utilizar una de sus computadoras para evitar pérdida, daños y modificación de la información con la que usted trabaja?		
9. ¿Cree usted que podría ocurrir un robo ocasionando pérdida o deterioro de su información la cual retrasaría o perjudicaría su trabajo?		
10. ¿En la institución educativa consideran las TIC para brindar una seguridad informática eficiente?		

Fuente: Elaboración Propia

DIMENSIÓN Nro. 02		
Encuesta para medir el nivel de satisfacción con respecto a la formación y capacitación a los Docentes, Personal Administrativo y Alumnos sobre el manejo de las TIC.		
PREGUNTAS	**SI**	**NO**
1. ¿Tiene conocimientos acerca de las herramientas TIC, en su institución?		
2. ¿Considera importante invertir en herramientas TIC para su institución?		
3. ¿Es bueno el nivel de las TIC en su Institución Educativa		
4. ¿Usted considera que los docentes de la institución educativa tienen un buen manejo de las TIC?		
5. ¿El gobierno, informa de manera correcta a las instituciones educativas en cuanto al manejo de las TIC?		
6. ¿Su institución realiza capacitaciones frecuentemente en temas de informática y tecnología?		
7. ¿Ha recibido capacitación útil por parte del área de computación de cómo proteger su información?		
8. ¿En la institución educativa existe una política de protección donde se les ha capacitado o formado en temas de seguridad informática a través de las TIC?		
9. ¿En su institución se implementan talleres de formación y preparación en temas seguridad y protección de información?		

10. ¿Siente que su institución se preocupa por capacitarlo en temas actuales de informática y tecnológicos?		

Fuente: Elaboración Propia

DIMENSIÓN Nro. 03		
Encuesta para medir el nivel de satisfacción con respecto a las TIC en el proceso de enseñanza aprendizaje.		
PREGUNTAS	**SI**	**NO**
1. ¿Considera usted que es necesaria la implementación de las TIC para un mejor rendimiento académico?		
2. ¿En su institución educativa se desarrollan las clases tomando en cuenta las herramientas TIC?		
3. ¿Se incorpora el uso de TIC en la práctica pedagógica, mediante la aplicación de investigaciones actualizadas sobre educación y uso de tecnología como marco referencia?		
4. ¿Considera que las TIC interactúan adecuadamente con los alumnos en el proceso de enseñanza?		
5. ¿Cree usted que se reflexiona respecto a los resultados y logros alcanzados en experiencias de aprendizaje desarrolladas con TIC actualizadas?		
6. ¿Se da seguimiento al proceso de aprendizaje de los alumnos utilizando las herramientas tecnológicas correspondientes y teniéndola bajo un rango de seguridad, dentro de su institución?		
7. ¿Usted cree que la institución considera que el uso de las herramientas TIC son buenas en el proceso de aprendizaje, y que estas necesiten de la seguridad informática?		

8. ¿Se seleccionan estrategias de aprendizaje con uso de herramientas de productividad (Word, Excel, Power Point entre otros) y recursos de Internet para diseñar un entorno de trabajo con los alumnos?		
9. ¿Se requiere de grupos de alumnos para encomendar materiales y tareas en actividades del proceso de aprendizaje utilizando recursos tecnológicos?		
10. ¿Se utilizan las TIC para la comunidad educativa en general con miras a intercambiar reflexiones, experiencias y productos que coadyuven a la actividad del docente y alumno?		

Fuente: Elaboración Propia

Anexo 04: Plan de taller de Capacitación

1) NOMBRE DEL TALLER:

"TALLER DE CAPACITACIÓN PARA EL MANEJO ADECUADO DE COMPETENCIAS TIC Y POLITICAS DE SEGURIDAD INFORMÁTICA"

2) LUGAR:

I.E. SAN MIGUEL ARCÁNGEL, CATACAOS – PIURA

3) TEMAS:

- EDUCACIÓN PARA EL MANEJO DE LAS TIC
- EDUCACIÓN DE TIC EN EL PROCESO ENSEÑANZA APRENDIZAJE.
- EDUCACIÓN DE POLITICAS DE SEGURIDAD INFORMÁTICA DENTRO DE LA I.E.

4) RESUMEN DEL CONTENIDO

Este taller es un espacio donde se combinaran dos partes importantes para el desarrollo de la mente, como lo es la teoría y la práctica, las cuales se unirán para poder llevar a cabo, por lo que actualmente la tecnología ya no solo se encuentra en grandes organizaciones sino también en las instituciones educativas. En la primera parte llevaremos a cabo la educación para el manejo de las TIC donde se les explicará las definiciones del software para luego proceder a la práctica explicándoles de una manera clara y concisa el manejo básico de estas. Como segunda parte tenemos la educación de las TIC como proceso de enseñanza y aprendizaje, logrando brindarle la información adecuada sobre el manejo de los diferentes programas instalados y puedan ser utilizados al momento de dictar sus

clases los docentes; y en lo que corresponde los alumnos poder hacer el desarrollo de actividades mediante estas herramientas de trabajo. Finalmente mostrarles las políticas de seguridad que están establecidas en la institución, brindándoles el manual correspondiente para que puedan tener más información, y explicándoles que se debe de realizar para poder tener segura nuestra información.

5) OBJETIVO

- Fomentar el uso y manejo adecuado de las TIC que se encuentran en la I.E. San Miguel Arcángel permitiendo la construcción de nuevos conocimientos para un mejor desarrollo de clases.

- Generar el trabajo colaborativo, grupal y se tenga en cuenta el intercambio de experiencias, llevando a mejorar el desempeño de los docentes para aportar en la mejora de la calidad del aprendizaje de los alumnos.

- Aportar conocimiento sobre los riesgos que existen en la institución si no se tiene en cuenta las políticas de seguridad informática.

6) MATERIAL Y EQUIPO

Infraestructura.- Para el desarrollo de las actividades de capacitación se tomaran en cuenta ambientes adecuados que sean proporcionados por la institución.

Mobiliario, equipo y otros.- Lo conforma las mesas de trabajo, sillas, pizarra, tizas, plumones, Proyector, TV, y ventilación adecuada.

Separatas Educativas.- Todo documento informativo como: Manual, certificados, encuestas de evaluación, material de estudio, etc.

7) PRESUPUESTO DEL TALLER DE CAPACITACIÓN

RUBRO	CANTIDAD	COSTO UNITARIO(S/.)	COSTO TOTAL (S/.)
MOVILIDAD			
Pasajes Catacaos centro hacia la I.E. y viceversa.	6 Pasajes	4.00	24.00
MATERIAL DE ESCRITORIO			
✓ Papelería	2 millar	12.00	48.00
✓ Lapiceros	02 unidades	0.50	1.00
✓ Folder	01 unidad	3.50	3.50
✓ Lápiz	01 unidad	1.00	1.00
✓ Cuaderno	01 unidad	12.00	12.00
✓ USB	01unidad	30.00	30.00
MATERIAL EDUCATIVO			
✓ Impresión	20 unidades	0.50	10.00
✓ Fotocopias	1500 unidades	0.10	150.00
		TOTAL	279.50

Fuente: Elaboración Propia

8) EVALUACIÓN

Los docentes, alumnos y personal administrativo al final tendrán una evaluación para poder certificar que el taller fue exitoso, verificaremos lo bueno y lo malo del taller y así precisar en qué podemos mejorar.