UNIVERSIDAD DE LAMBAYEQUE

FACULTAD DE CIENCIAS DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TRABAJO DE INVESTIGACIÓN

ANÁLISIS DE SEGURIDAD INFORMÁTICA DE LOS ACTIVOS EN LA INSTITUCIÓN EDUCATIVA SECUNDARIA POLITÉCNICO "PEDRO ABEL LABARTHE DURAND", CHICLAYO, 2019

AUTOR:
PEDRAZA ALBURQUERQUE ELMER GABRIEL

PRESENTADO COMO REQUISITO PARCIAL PARA OPTAR EL GRADO DE BACHILLER EN INGENIERÍA DE SISTEMAS

Chiclayo - Perú
2019

Dedicatoria

Dedico este trabajo a Dios,
por ser el creador de
todas las cosas,
y a mis padres por ser,
mis primeros maestros
y mi razón de ser.

Agradecimiento

A mi familia, por su comprensión y estimulo constante, además de su apoyo incondicional a lo largo de mis estudios.

A mi asesor: Mg Torres Nauca Enrique Santos, quien me brindo su valiosa y desinteresada orientación y guía en la elaboración del presente trabajo de investigación.

Y a todas las personas que en una u otra forma me apoyaron en la realización de este trabajo.

Resumen

La seguridad informática es una dificultad constante en todas las organizaciones públicas y privadas. Aunque algunas ya han tomado conciencia de esta problemática, muchas otras aún no participan de la cultura de la seguridad informática. Dentro de este segundo grupo de organizaciones se encuentra la I.E Secundaria Politécnico "Pedro Abel Labarthe Durand". Teniendo un serio peligro la información que se gestiona y administra.

Mediante este trabajo de investigación se inició con una encuesta, a modo de diagnóstico, acerca de la situación actual de la seguridad informática, en la cual se identificó factores de riesgos que afectan a los activos de la I.E Pedro Abel Labarthe Durand. Mediante los resultados de la encuesta realizada a los colaboradores se llegó a detectar varias deficiencias y factores de riesgos, ya que no cuenta con capacitaciones e información en el área de AIP(cómputo).

Palabras Claves: Seguridad informática, cultura de la seguridad informática, factores de riesgos.

Índice

Índice de tablas

Índice de figuras

I. Problema de investigación

Según Mendoza, A (2016), 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.

Al haber realizado el análisis a la seguridad de información, se pudo identificar diferentes tipos de riesgos, vulnerabilidades, fallas, que puedan presentarse en la institución educativa Pedro Abel Labarthe Durand, se necesitó información de la vulnerabilidad existentes y de la seguridad d información.

La Institución Educativa Pedro Abel Labarthe Durand, maneja una base de datos de los alumnos matriculados, que es llevado en una plataforma, y para el manejo de registro de notas, se realiza con otra plataforma, que es administrada por la secretaria.

La institución educativa Pedro Abel Labarthe Durand, cuenta con 2 sedes en áreas, encontrándose una en Colon 259, Chiclayo 14001, y la otra en Pimentel 88, Chiclayo 14012, donde no hay casi disponibilidad. Se tuvo como problema de investigación: ¿De qué manera un análisis de Seguridad de informática permite identificar vulnerabilidades en los activos de la institución educativa "Pedro Abel Labarthe Durand"?, teniendo como objetivo principal: Analizar la seguridad informática de los activos en la Institución educativa secundaria Politécnico "Pedro Abel Labarthe Durand", Chiclayo , y también conto con objetivos específicos: (1) Conocer la situación actual de la seguridad informática dentro de la Institución educativa "Pedro Abel Labarthe Durand", (2) Identificar los factores de riesgos de los activos de la Institución educativa "Pedro Abel Labarthe Durand" y como justificación el desarrollo avanzado de la tecnología, ha ocasionado graves dificultades de vulnerabilidad en las organizaciones, con riesgos e inseguridad.

Mediante este trabajo de investigación en la I.E Politécnico "Pedro Abel Labarthe Durand", se tomaron medidas de prevención de seguridad para evitar que la información sea sustraída o alteradas por terceros con la finalidad de minimizar las amenazas y tratas de mantener la confidencialidad, integridad y disponibilidad de la información.

La Institución educativa Secundaria Politécnico" Pedro Abel Labarthe Durand" necesitan de un Análisis de Seguridad informática de los activos, en la cual nos permita saber si el sistema de información se encuentra protegida de cualquier tipo de amenazas internas o externas.

II. Marco teórico y metodológico

2.1. Antecedentes bibliográficos

Según Bermúdez Molina y Bailón Sánchez (2015),en su tesis titulada "Análisis en seguridad informática y seguridad en la información basado en la norma ISO/IEC 27001- sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros, mediante la elaboración del análisis de seguridad de la información y seguridad informática basada en la norma ISO/TEC 27001", el presente trabajo tuvo como finalidad conocer las vulnerabilidades a las que esta expuesta la información por la falta de aplicación de controles de seguridad.

El análisis estubo dirgido a una empresa financiera, teniendo como objetivo principal el estudio de seguridad en los procesos críticos. A través de reuniones, revisión de documentación, consultas, observación, encuestas y ejecución de entrevistas con directivos que poseen un amplio conocimiento del negocio, se logró identificar los riesgos actuales a los que se exponen los datos tanto físicos, lógicos y sistemas de procesamiento de información

Los resultados obtenidos dan a conocer que, para minimizar los riesgos existentes, es necesario implementar controles de seguridad, lo cual ayuda a fortalecer tres aspectos importantes: la confidencialidad, integridad y disponiblidad de la información. Pero los resultados también muestran la importancia del compromiso y trabajo en equipo que debe tener la empresa.

Según Gonzáles Retamozo (2017), con su proyecto de tesis titulada "Auditoría de seguridad informática para la Institución Educativa Departamental Luis Carlos Galán - municipio de yacopí cundinamarca", nos habla que la Institución Educativa Departamental Luis Carlos Galán, maneja una base de datos de los alumnos matriculados, que es llevado en la plataforma SIMAT, que es administrada por la Secretaria de Educación Nacional, y para el manejo de registro de notas, se realiza con otra plataforma llamada SIGES, que es administrada por la secretaria de educación de Cundinamarca; este último, ha tenido en sus últimos años dificultades con su sistema de información de registro de notas, como por la suplantación de usuarios al sistema, para eso plantea un objetivo general Disminuir las vulnerabilidades y amenazas de seguridad en el registro académico y de notas de los estudiantes con la auditoria del sistema de gestión de seguridad de la información para la institución educativa departamental Luis Carlos Galán del municipio de Yacopí – Cundinamarca.

Por esta razón la institución deberá implementar una auditoria al sistema de seguridad informático e implementar un plan de mejoramiento con las politicas de seguridad.

Según Guamán Seis Joseph Alexander (2015), en la tesis titulada "Diseño de un Sistema de Gestion de Seguridad de la Información para Instituciones Militares", el presente trabajo de tesis tiene como objetivo principal Diseñar un Sistema de Gestión de Seguridad de la Información para Instituciones Militares, que incorpore estándares internacionales ajustados al campo militar y nuevas tecnologías de la información y comunicaciones con el fín de contribuir a la modernización de las Instituciones Militares, tomando como caso de estudio en la Armada del Ecuador a la Dirección de Tecnologías de la Información y Comunicaciones.

Se desarrollo bajo la modalidad de estudios de proyecto apoyado tanto en una investigación de campo como en la investigación monográfica documental que permitió la elaboración y desarrollo de una propuesta de un modelo operativo viable para solventar los problemas de seguridad de la información de las Instituciones Militares y de la Dirección de Tecnologías de la Información y Comunicaciones.

Según Ancajima (2016), en su informe de investigación sobre la información y comunicación (TIC), para la mejora contínua 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; 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. 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.

Según Chura Coqueña (2018) , en la tesis titulada "Plan de Seguridad Informática en la Municipalidad Provincial de San Román (Sistema Web)", nos dice que la seguridad de la información es un conjunto de procesos, procedimientos, tareas y actividades implementados conjuntamente con elementos de computación y telecomunicaciones para controlar y proteger contra amenazas que pongan en riesgo los recursos informáticos (información, equipos, etc.) ubicados en un sitio específico, durante su estadía en un medio de almacenamiento o durante su transmisión, en sus aspectos de integridad, disponibilidad, confidencialidad y autenticidad. Para lo

cual el presente trabajo de investigación que se realizó, Plan de Seguridad Informática en la Municipalidad Provincial de San Román (Sistema Web). Para lograr dicho propósito se formuló un objetivo general que es Proponer un plan de seguridad informática para internet en la municipalidad provincial de San Román. Así mismo se realizó el estudio con una población siendo el universo, que es un conjunto de personas y una muestra que se determina atreves del método provistico siendo elegido un total de población de forma sistémica. La conclusión del presente trabajo de investigación refiere de acuerdo a los resultados que se han obtenido es con respecto a la percepción de la dimensión de paradigmas con un total de deficiencia de un 99%.

Según Gonzáles Sosa, Henry Jesus y Delgado Flores, Ismael (2018), en la tesis titulada "Diseño del plan de contingencia como herramienta para gestionar riesgos de la seguridad de la información en el área del centro de sistemas de información de la Ugel-Ferreñafe en el periodo 2018", nos habla que este diseño servirá como guía para que el responsable del área de (CSI), tome las medidas pertinentes para la mitigación de los riesgos a los que se encuentra expuestos los activos de la Ugel – Ferreñafe; dentro de la investigación podrá tener conocimiento de los activos críticos y/o personas o procesos que la involucren. Su objetivo principal es elaborar el Plan de Contingencia como herramienta para la Gestión de los Riesgos de la seguridad de la información en el área del centro de sistemas de información de la UGEL-FERREÑAFE en el periodo 2018.

El Diseño del plan de contingencia será un factor relevante para afrontar de manera oportuna, adecuada y efectiva la eventualidad de incidentes, accidentes y/o estados de emergencias que pudiera sufrir el área de CSI de la Ugel – Ferreñafe, su uso permitirá optimizar los recursos tanto humanos como materiales.

A través de esta investigación se dará a conocer las acciones a tomar para prevenir las brechas de seguridad a las que se encuentra expuesta el área de CSI de la Ugel – Ferreñafe, muchas de ellas son de carácter educativo las cuales se cubrían con solo capacitar al empleador en temas de seguridad

2.2. Materiales y métodos:

2.2.1 Tipo de estudio y diseño de investigación

2.2.1.1 Tipo de estudio

El tipo de investigación será descriptiva según Cazau, P (2006), nos habla que el estudio descriptivo se seleccionan una serie de cuestiones, conceptos o variables y se mide cada una de ellas independientemente de las otras, con el fín,

precisamente, de describirlas. Estos estudios buscan especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno.

2.2.1.2 Diseño de investigación

El diseño de investigación será no experimental según Hernandez, Fernandez y Baptista (1991), nos dice que la investigación no experimental es también conocida como investigación Ex Post Facto, donde los cambios en la variable independiente ya ocurrieron y el investigador tiene que limitarse a la observación de situaciones ya existentes dada la incapacidad de influir sobre las variables y sus efectos"

2.2.2 Variables del estudio

2.2.2.1 Variable única

Seguridad Informática

2.2.3 Hipótesis

Por ser tipo de investigación descriptiva la hipótesis es opcional.

2.2.4 Población y Muestra de estudio:

2.2.4.1 Población:

La población estará conformada 3 colaboradores de la I.E Pedro Abel Labarthe Durand.

Tabla 1

Número de colaboradores

Detalle	Cantidad
Director	1
Administración	1
Centro AIP	1
Total	3

Fuente 1: Documentación de colaboradores

2.2.4.2 Muestra:

Conformada por la misma población

2.2.5 Métodos, técnicas e instrumentos de recolección de datos

2.2.5.1 Técnica

a) Encuesta

Según Casas, Repullo y Donado (2003), nos dice que la técnica de encuesta es ampliamente utilizada como procedimiento de investigación, ya que permite obtener y elaborar datos de modo rápido y eficaz.

Esta encuesta fue dirigida al Director Calle Olemar Juan Carlos , Docente AIP Berrios Sanchez Merly, Docente Administrativo Palacios Felicitas Malca.

b) Entrevista

Según Díaz, Torruco, Martínez y Varela (2013), nos dice que la entrevista es una técnica de gran utilidad en la investigación cualitativa para recabar datos; se define como una conversación que se propone un fín determinado distinto al simple hecho de conversar. Es un instrumento técnico que adopta la forma de un diálogo coloquial. Canales la define como "la comunicación interpersonal establecida entre el investigador y el sujeto de estudio, a fín de obtener respuestas verbales a las interrogantes planteadas sobre el problema propuesto".

Esta entrevista fue dirigida al Director Calle Olemar Juan Carlos , Docente AIP Berrios Sanchez Merly, Docente Administrativo Palacios Felicitas Malca.

c) Observación

Según Díaz (2011), nos habla que la observación es un elemento fundamental de todo proceso de investigación; en ella se apoya el investigador para obtener el mayor número de datos. Gran parte del acervo de conocimientos que constituye la ciencia ha sido lograda mediante la observación. La observación está influida por el marco(s) teórico(s) que ha aprendido el psicólogo, y que partiendo del mismo, va a influir en esa forma de observación que inicia el proceso de conocimiento de la persona que acude para ser diagnosticada y posteriormente intervenida.

2.2.5.2 Instrumento

a) Cuestionario

Según Meneses y Rodríguez (2011), nos habla que el cuestionario es, por definición, el instrumento estandarizado que utilizamos para la recogida de datos durante el trabajo de campo de algunas investigaciones cuantitativas, fundamentalmente, las que se llevan a cabo con metodologías de encuestas. En pocas palabras, se podría decir que es la herramienta que permite al científico social

plantear un conjunto de preguntas para recoger información estructurada sobre una muestra de personas, utilizando el tratamiento cuantitativo y agregado de las respuestas para describir la población a la que pertenecen o contrastar estadísticamente algunas relaciones entre variables de su interés. Así, si el cuestionario es la técnica o instrumento utilizado, la metodología de encuestas es el conjunto de pasos organizados para su diseño y administración y para la recogida de los datos obtenidos. La distinción es importante, aunque no es infrecuente encontrar un cierto intercambio entre estos términos, utilizando la palabra encuesta para referirse también a un cuestionario específico. Más allá de la precisión terminológica, lo que es realmente importante es tener presente la diferencia fundamental existente entre el método de investigación que nos provee del contexto para tomar decisiones en el diseño de la investigación con cuestionarios, y la herramienta que el científico elabora para llevar a cabo su recogida de datos durante el trabajo de campo.

b) Guía de entrevista

Según Ortíz (2015), es un documento que contiene los temas, preguntas sugeridas y aspectos a analizar en una entrevista.

Dentro de los temas que se encuentran: Experiencia profesional, estudios y formación, historia familiar entre otros, esto nos es útil para reorganizar expectativas, responsabilidades, fomentar una atmósfera cálida de aceptación, confianza y empatía.

c) Guía de observación

Según Ortíz (2015), una guía de observación, por lo tanto, es un documento que permite encausar la acción de observar ciertos fenómenos.

Esta guía, por lo general, se estructura a través de columnas que favorecen la organización de los datos recogidos.

2.2.6 Procesamiento de datos y análisis estadístico

Para el reciente estudio se empleará las técnicas de entrevista y encuestas que tiene como instrumento el cuestionario, que estará dirigida a la Institución Educativa “Pedro Abel Labarthe Durand “que resulten seleccionados en la muestra del estudio. Para ello se realizará la tabulación en tablas y figuras con la herramienta Microsoft Excel

III. Resultados

3.1 Conocer la situación actual de la seguridad informática dentro de la Institución educativa "Pedro Abel Labarthe Durand"

a) Encuesta: El análisis de encuesta fue brindada hacia los colaboradores ya que eso nos ayudará a saber si su sistema de información se encuentra segura en la Institución Educativa "Pedro Abel Labarthe Durand.

Tabla 2

Existen revisiones periódicas de Hardware y Software

Categoría	Frecuencia	Porcentual
SI	1	33%
NO	2	67%
Total	3	100%

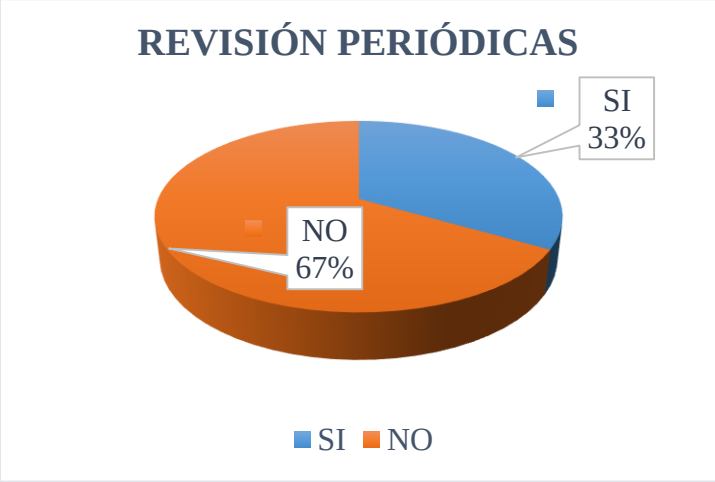


Figura 1. Existen revisiones periódicas de Hardware y Software

Fuente: Encuesta a los colaboradores de la I.E Politécnico "Pedro Abel Labarthe Durand"

Interpretación

Según los resultados un 67% respondieron, ya siendo un porcentaje muy elevado nos dice que no existen revisiones periódicas de Hardware y Software, mientras que un 33% respondieron que si hacen de vez en cuando.

Tabla 3

A su criterio ¿Conoce normas o procedimientos legales para la seguridad de la información?

Categoría	Frecuencia	Porcentual
SI	3	100%
NO	0	0%
Total	**3**	**100%**

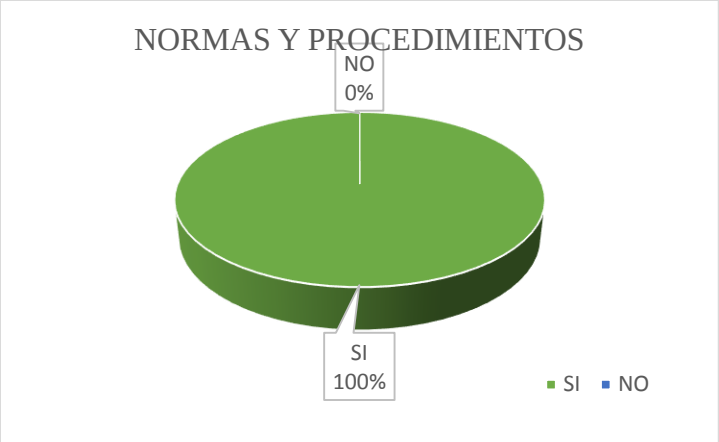


Figura 2. A su criterio, ¿Conoce normas o procedimientos legales para la seguridad de la información?

Fuente*:* Encuesta a los colaboradores de la I.E Politécnico "Pedro Abel Labarthe Durand"

Interpretación

Mediante la figura se puede apreciar que el 100% de colaboradores conocen normas o procedimientos legales para la seguridad de la información.

Tabla 4

Conoce Ud. ¿Si existen políticas de seguridad para la información en el centro de sistemas de la información (CSI) de la UGEL?

Categoría	Frecuencia	Porcentual
SI	1	33%
NO	2	67%
Total	**3**	**100%**

Figura 3. Conoce Ud. ¿Si existen políticas de seguridad para la información en el centro de sistemas de la información (CSI) de la UGEL?

Fuente: Encuesta a los colaboradores de la I.E Politécnico "Pedro Abel Labarthe Durand"

Interpretación

Del total de los encuestados el 67% no conoce que existan políticas de seguridad para la información en el centro de sistemas de información (CSI), en tanto que en un menor porcentaje de 33% si conoce.

Tabla 5

A su criterio. ¿Existe un personal encargado en atender y rectificar los incidentes ocasionados por las amenazas de la seguridad de información?

Categoría	Frecuencia	Porcentual
SI	2	67%
NO	1	33%
Total	**3**	**100%**

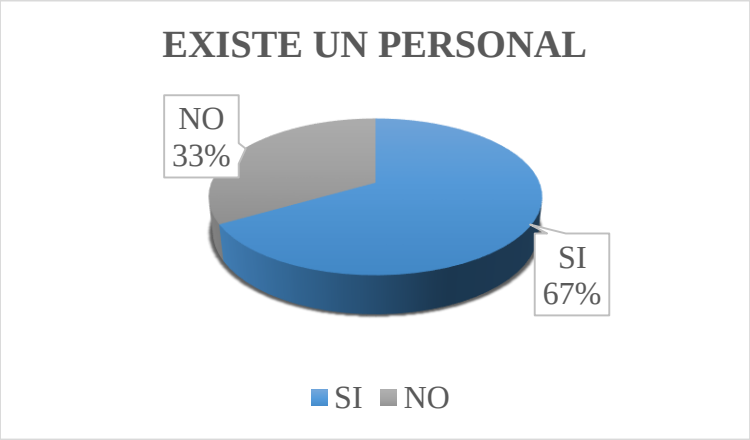


Figura 4. A su criterio. ¿Existe un personal encargado en atender y rectificar los incidentes ocasionados por las amenazas de la seguridad de información?

Fuente: Encuesta a los colaboradores de la I.E Politécnico "Pedro Abel Labarthe Durand"

Interpretación

Mediante la figura se puede apreciar que el 67% de los encuestados menciona que si existe personal encargado de atender y corregir los incidentes por amenazas de la seguridad de la información; y un 33% menciona que no existe.

Tabla 6

¿La información que usted utiliza, se encuentra protegida?

Categoría	Frecuencia	Porcentual
SI	1	33%
NO	2	67%
Total	**3**	**100%**

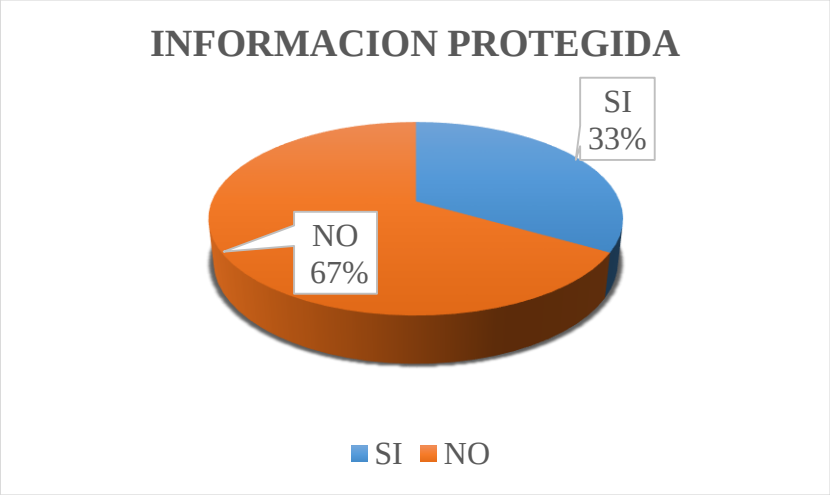


Figura 5. ¿La información que usted utiliza, se encuentra protegida?

Fuente: Encuesta a los colaboradores de la I.E Politécnico "Pedro Abel Labarthe Durand"

Interpretación

Se aprecia que el 67% de los colaboradores menciona que la información que se utiliza no se encuentra protegida; en tanto que en un menor porcentaje de 33% menciona que si se encuentra protegida

Tabla 7

¿La seguridad respecto al software, se encuentra protegida?

Categoría	Frecuencia	Porcentual
SI	1	33%
NO	2	67%
Total	**3**	**100%**

Figura 6. ¿La seguridad respecto al software, se encuentra protegida?

Fuente: Encuesta a los colaboradores de la I.E Politécnico "Pedro Abel Labarthe Durand"

Interpretación

Del total de los encuestados el 67% respondieron que la seguridad respecto al Software no se encuentra protegida, mientras que un 33% respondieron que si se encuentra protegida

Tabla 8

¿Está de acuerdo que aprueben medidas de seguridad en la UGEL?

Categoría	Frecuencia	Porcentual
SI	3	100%
NO	0	0%
Total	**3**	**100%**

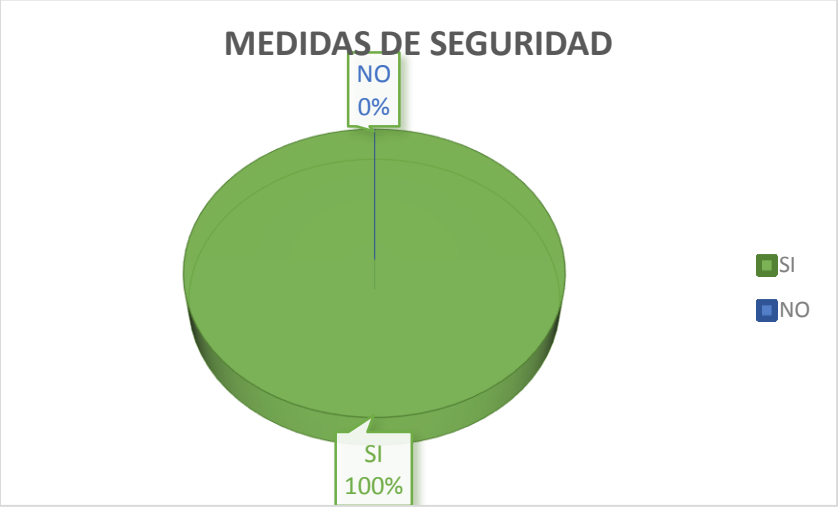


Figura 7. ¿Está de acuerdo que se aprueben medida de seguridad en la UGEL?

Fuente: Encuesta a los colaboradores de la I.E Politécnico "Pedro Abel Labarthe Durand"

Interpretación

Se puede apreciar que del 100% de los colaboradores el 100% respondieron que si están de acuerdo que se aprueben medidas de seguridad en la UGEL.

Tabla 9

Según Ud. ¿Se debería monitorear y evaluar los procesos de contingencia y restauración implementados en la UGEL?

Categoría	Frecuencia	Porcentual
SI	3	100%
NO	0	0%
Total	**3**	**100%**

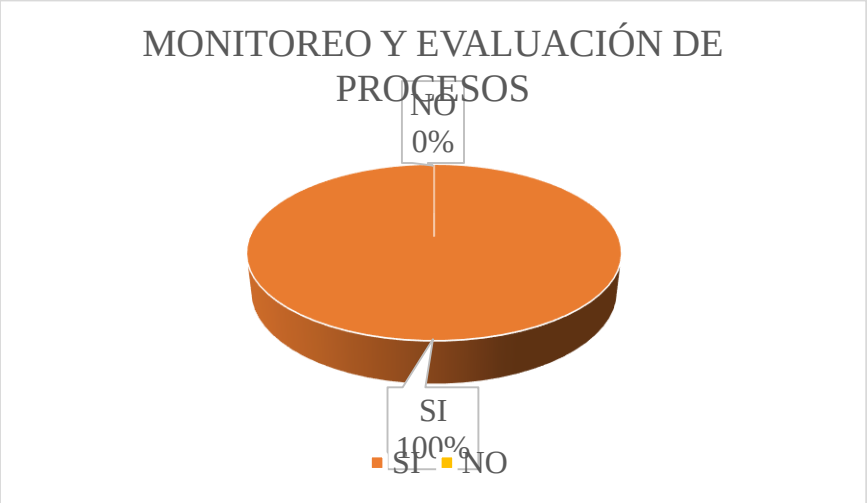


Figura 8. Según Ud. ¿Se debería monitorear y evaluar los procesos de contingencia y restauración implementados en la UGEL?

Fuente: Encuesta a los colaboradores de la I.E Politécnico "Pedro Abel Labarthe Durand"

Interpretación

Del total de los encuestados el 100% respondieron que sí se debería monitorear y evaluar los procesos de contingencia y restauración implementado en la UGEL.

Tabla 10

¿Alguna vez se le hizo la entrega de algún tipo de documento o plan de seguridad de la información?

Categoría	Frecuencia	Porcentual
SI	1	33%
NO	2	67%
Total	**3**	**100%**

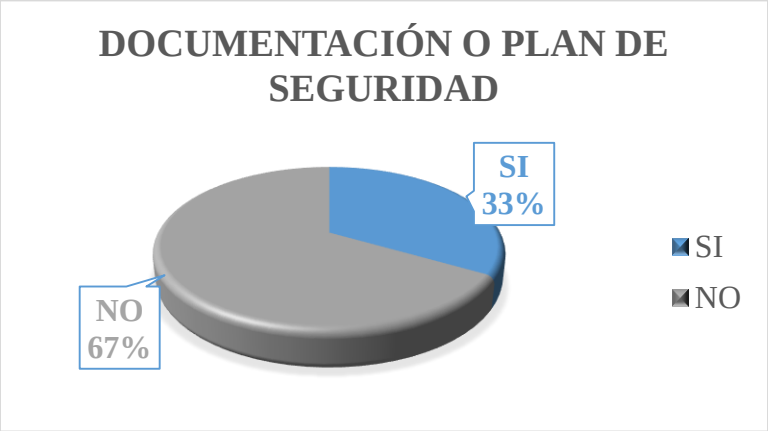


Figura 9. ¿Alguna vez se le hizo la entrega de algún tipo de documento o plan de seguridad de la información?

***Fuente*:** Encuesta a los colaboradores de la I.E Politécnico "Pedro Abel Labarthe Durand"

Interpretación

Del total de los colaboradores encuestados el 67% respondieron que no se le hizo entrega de algún tipo de documento o plan de seguridad de la información y un 33% nos respondieron que si alguna vez se hizo entrega.

Tabla 11

¿Se mantiene programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otro equipo?

Categoría	Frecuencia	Porcentual
SI	1	33%
NO	2	67%
Total	**3**	**100%**

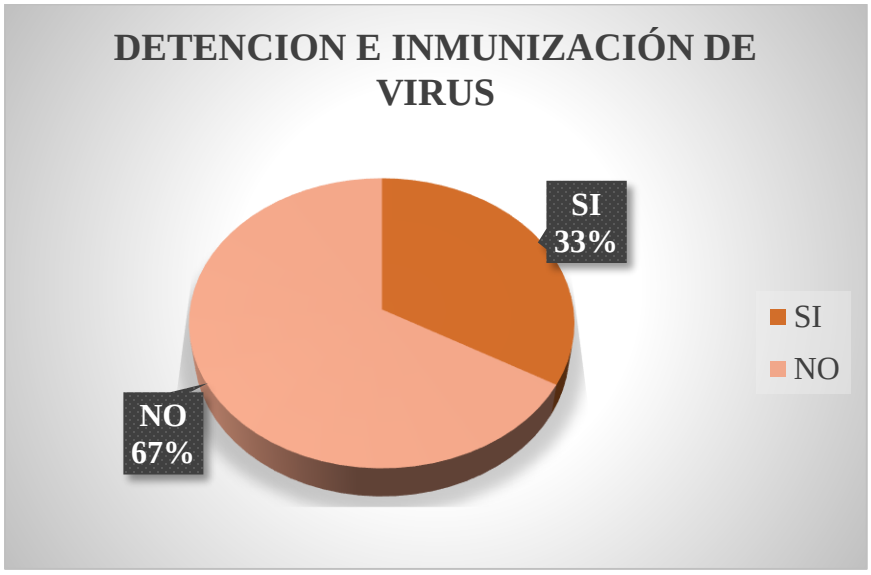


Figura 10. ¿Se mantiene programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otro equipo?

Fuente: Encuesta a los colaboradores de la I.E Politécnico "Pedro Abel Labarthe Durand"

Interpretación

Se puede apreciar que a nivel general el 67% respondieron que no se mantiene programas y procedimientos de detección de inmunización de virus en copias no autorizadas o datos procesados en otro equipo, mientras que el 33% respondieron que sí.

3.2 Identificar los factores de riesgos de los activos de la Institución educativa "Pedro Abel Labarthe Durand".

b) Observación: Se hizo observaciones al área de AIP para determinar los factores en riesgos.

1- Los enrutadores están en un lugar seguro.

Figura 11. Los enrutadores están en un lugar seguro

Interpretación

Según a lo apreciado se notó que su enrutador si se encuentra en un lugar seguro, donde no pueda incomodar y pueda ser más fácil de hacer conexiones

2- Los cables de red están protegidos con canaletas.

Figura 12. Los cables de red están protegidos con canaletas

Interpretación

De acuerdo a la observación se vió que los cableados cuentan con canaletas anchas para ser protegidos de cualquier incidente

3- Los terminales (PC) tienen contraseñas.

Figura 13. Los terminales (PC) tienen contraseñas

Interpretación

Según a lo apreciado se notó que los terminales(PC) si cuentan con contraseñas a la hora de iniciar sesión.

4- Los equipos informáticos están en buen estado.

Figura 14. Los equipos informáticos están en buen estado

Interpretación

En dicha observación que se hizo se percibió que los equipos informáticos se encuentran en buen estado, se mantienen limpias y en una posición adecuada

5- Los terminales (PC), cuentan con antivirus.

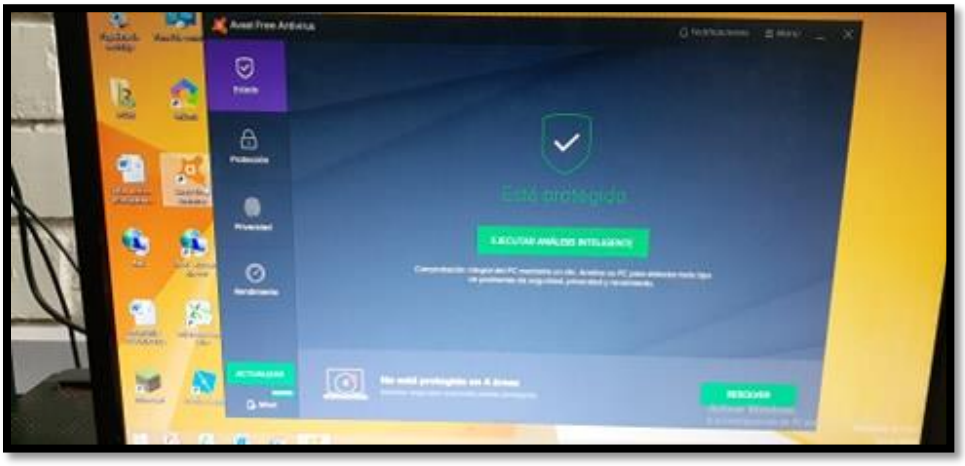


Figura 15. Los terminales (PC), cuentan con antivirus

Interpretación

Según a la observación que se hizo se percibió que los terminales (PC), cuentan con un antivirus que es de software libre

6- Los equipos informáticos están conectados a UPS.

Figura 16. Los equipos informáticos están conectados a UPS

Interpretación

Se pudo apreciar que los equipos informáticos no se encuentran conectados a un UPS.

7- Cuentan con un protocolo de seguridad para la protección de los equipos informáticos.

Figura 17. Cuentan con un protocolo de seguridad para la protección de los equipos informáticos

Interpretación

Se pudo apreciar que no cuentan con un protocolo de seguridad para la protección de sus equipos informáticos

V. Discusión

Al conocer la situación actual de la seguridad informática dentro de la Institución, se pudo constatar en la recopilación de información en que los usuarios manifestaron que los sistemas de información tienen un nivel bajo en seguridad y además se tiene una bajo índice en las revisiones periódicas del hardware y también no se tiene un antivirus actualizado , que por ende es muy necesario para resguardar la información que es relevante para organización, en el cual lo manifiesta Bermúdez Molina y Bailón Sánchez (2015),en su tesis titulada "Análisis en seguridad informática y seguridad en la información basado en la norma ISO/IEC 27001- sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros, mediante la elaboración del análisis de seguridad de la información y seguridad informática basada en la norma ISO/TEC 27001", el presente trabajo tuvo como finalidad conocer las vulnerabilidades a las que esta expuesta la información por la falta de aplicación de controles de seguridad.

Al Identificar los factores de riesgos de los activos de la Institución, se pudo corroborar que los equipos informáticos no se encuentran conectados a ningún UPS en la cual durante un apagón eléctrico puede proporcionar energía eléctrica por un tiempo limitado a todos los dispositivos que tenga conectados y, además no cuentan con un protocolo de seguridad para la protección de los equipos informáticos, en lo cual lo manifiesta Chura Coqueña (2018) , en la tesis titulada "Plan de Seguridad Informática en la Municipalidad Provincial de San Román (Sistema Web)", nos dice que la seguridad de la información es un conjunto de procesos, procedimientos, tareas y actividades implementados conjuntamente con elementos de computación y telecomunicaciones para controlar y proteger contra amenazas que pongan en riesgo los recursos informáticos (información, equipos, etc.) ubicados en un sitio específico, durante su estadía en un medio de almacenamiento o durante su transmisión, en sus aspectos de integridad, disponibilidad, confidencialidad y autenticidad.

VI. Conclusiones

- De acuerdo a nuestras encuestas aplicadas en la Institución Educativa Politécnico ”Pedro Abel Labarthe Durand”, se pudo concluir que las entidades no están capacitadas para poder enfrentar algún tipo de amenazas de la seguridad de la información de sus activos, hace falta de capacitaciones, evaluaciones mensuales o semanales de los riesgos sobre los activos de información y dando a resultado de la encuesta sobre revisiones periódicas de Hardware y Software nos muestran un 67% respondieron que no existen revisiones y un 33% que sí , también nos habla que si existen políticas de seguridad para la información el centro de sistemas de la información (CSI) de la Ugel nos muestra un 67% respondieron que no conocen las políticas de seguridad para la información y un 33% nos respondieron que si conocen y en lo que es la Seguridad Informática y de Software nos muestra según los resultados un 67% que la información y la seguridad respecto al Software no se encuentran protegidas y un 33% que si se encuentran protegidas de cualquier tipo de factores de riesgos.
- De acuerdo a la ficha de observación planteada se pudo concluir que los equipos informáticos no se encuentran conectados con algún tipo de UPS, ni tampoco cuentan con un protocolo de seguridad para la protección de los equipos informáticos, ya que ese protocolo recopila serie de pautas y lineamientos de seguridad, cuya finalidad es la prevención de accidentes de trabajo.

VII. Recomendaciones

- Se recomienda hacer evaluaciones mensuales o semanales de cada área de sistema de información con el propósito de prevenir fallos o riesgos.
- Se recomienda mayor capacitación e información a todas las áreas, sobre todo en el área de AIP de temas coherentes a factores de riesgos y seguridad de la información.
- Se le recomienda para mayor seguridad de información, que los equipos sean conectados a un servidor UPS.

- Se le recomienda que cuenten con un protocolo de seguridad para la protección de los equipos informáticos.
- Se recomienda que cuenten con programas y procedimientos de detección de virus en copias no autorizadas o datos procesados en otro equipo.

VIII. Referencias bibliográficas

Ancajima, M. (2016). PROPUESTA DE IMPLEMENTACIÓN DE SEGURIDAD INFORMÁTICA EN LAS TIC DE LA I.E. SAN MIGUEL ARCÁNGEL, CATACAOS - PIURA; 2016. Piura, Peru. Retrieved from file:///E:/BACHILLER/bachiller%20tesistas/otro-CONTROL_SEGURIDAD_ANCAJIMA_MENDOZA_MARIA_ALEJANDRA.pdf

Bermudez Molina; Bailon Sanchez;. (2015). ANALISIS EN SEGURIDAD INFORMATICA Y SEGURIDAD DE LA INFORMACION BASADO EN LA NORMA ISO/IEC 27001-SISTEMAS DE GESTION DE SEGURIDAD DE LA INFORMACION DIRIGIDO A UNA EMRPESA DE SERVICIOS FINANCIEROS. Guayaquil, Ecuador. Retrieved from https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf

Casas, A; Repullo, L; Donado, C;. (2003). La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos (I). Madrid, España. Retrieved from https://www.elsevier.es/es-revista-atencion-primaria-27-articulo-la-encuesta-como-tecnica-investigacion--13047738

Cazau, P;. (2006). INTRODUCCIÓN A LA INVESTIGACIÓN EN CIENCIAS SOCIALES. Buenos Aires. Retrieved from http://alcazaba.unex.es/asg/400758/MATERIALES/INTRODUCCI%C3%93N%20A%20LA%20INVESTIGACI%C3%93N%20EN%20CC.SS..pdf

Celis, L;. (2018). PLAN DE SEGURIDAD DE LA INFORMACIÓN APLICADO A LA CENTRAL HIDROELÉCTRICA CARHUAQUERO. chiclayo, Peru. Retrieved from file:///H:/BACHILLER/bachiller%20tesistas/TL_CelisFigueroaLeonardo.pdf

Chura , E;. (2018). PLAN DE SEGURIDAD INFORMÁTICA EN LA MUNICIPALIDAD PROVINCIAL DE SAN ROMÁN (SISTEMA WEB). Juliaca, Peru. Retrieved from file:///H:/BACHILLER/bachiller%20tesistas/T036_24007013.pdf

Chura Coqueña, Edgar Wilsaac. (2018). PLAN DE SEGURIDAD INFORMÁTICA EN LA. U N I V E R S I D A D A N D I N A, INGENIERÍA DE SISTEMAS, Juliaca. Retrieved 2019

Diaz, L;. (2011). LA OBSERVACION. Mexico. Retrieved from http://www.psicologia.unam.mx/documentos/pdf/publicaciones/La_observacion_Lidia_Diaz_Sanjuan_Texto_Apoyo_Didactico_Metodo_Clinico_3_Sem.pdf

Diaz, L; Torruco, U; Martinez , M; Varela, M;. (2013). Metodología de investigación en educación médica. Mexico. Retrieved from http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-50572013000300009

Gonzales Retamozo;. (2017). AUDITORIA DE SEGURIDAD INFORMÁTICA PARA LA INSTITUCIÓN EDUCATIVA DEPARTAMENTAL LUIS CARLOS GALÁN - MUNICIPIO DE YACOPÍ CUNDINAMARCA. Dorada-Caldas, Colombia. Retrieved from file:///H:/BACHILLER/bachiller%20tesistas/10188295.pdf

Gonzales Sosa, Henry Jesus y Delgado Flores, Ismael;. (2018). Diseño del plan de contingencia como herramienta para gestionar riesgos de la seguridad de la informacion en el area centro de sistemas de informacion de la UGEL-Ferreñafe en el periodo 2018. Ferreñafe, Peru. Retrieved from http://repositorio.udl.edu.pe/handle/UDL/235

Guaman , J;. (2015). DISEÑO DE UN SISTEMAS DE GESTION DE SEGURIDAD DE LA INFORMACION PARA INSTITUCIONES MILITARES. Quito, Ecuador. Retrieved from file:///H:/%C2%A0/TRABAJOS%20DECIMO/BACHILLER/OTRO-CD-6187.pdf

Guaman Seis , Joseph Alexander;. (2015). DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA INSTITUCIONES MILITARES. Quito, Ecuador. Retrieved from file:///H:/BACHILLER/bachiller%20tesistas/OTRO-CD-6187.pdf

Guzman , G;. (2015). METODOLOGÍA PARA LA SEGURIDAD DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES EN LA CLÍNICA ORTEGA. Huancayo, Peru. Retrieved from http://repositorio.uncp.edu.pe/bitstream/handle/UNCP/1478/Tesis-Goyo%20Francisco%20Guzman%20Pacheco.pdf?sequence=1&isAllowed=y

Hernandez, S; Fernandez, C; Baptista, P;. (1991). METOLOGIA DE LA INVESTIGACION. Mexico. Retrieved from http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdf

Mendoza, A. (2016). PROPUESTA DE IMPLEMENTACIÓN DE SEGURIDAD INFORMÁTICA EN LAS TIC DE LA I.E. SAN MIGUEL ARCÁNGEL, CATACAOS - PIURA; 2016. Piura. Retrieved from file:///C:/Users/Gabriel/Documents/PRACTICAS%204%20EDGAR/BACHILLER/otro-CONTROL_SEGURIDAD_ANCAJIMA_MENDOZA_MARIA_ALEJANDRA.pdf

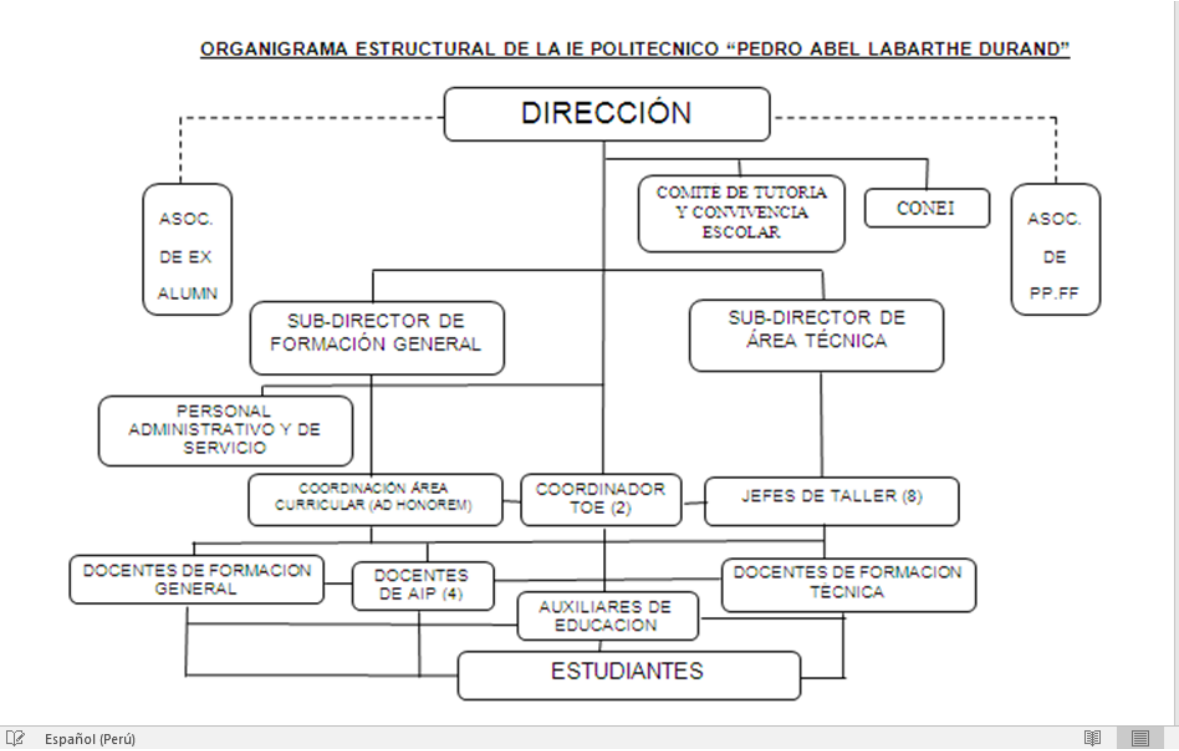
Meneses , J; Rodriguez, D;. (2011). El cuestionario y la entrevista. Barcelona. Retrieved from http://femrecerca.cat/meneses/files/pid_00174026.pdf

Ortiz, M;. (2015). Guia de entrevista y de observación. Peru. Retrieved from https://prezi.com/ooatecj5_fgt/guia-de-entrevista-y-de-observacion/

Ortiz, M;. (2015). Guia de entrevista y de observación. Peru. Retrieved from https://prezi.com/ooatecj5_fgt/guia-de-entrevista-y-de-observacion/

IX. Anexos

A01: Organigrama de la I.E Politécnico" Pedro Abel Labarthe Durand"



A02: Población y muestra de estudio

POBLACIÓN	DESCRIPCIÓN
1. Juan Carlos Calle Olemar	Lic. En Educación
2. Merly Berrios Sánchez	Magister
3. Malca Palacios Felicitas	Administrativa

FICHA DE OBSERVACIÓN

PREGUNTAS:	SI	NO
Los enrutadores están en un lugar seguro	X	
Los cables de red están protegidos con canaletas.	X	
Los terminales (PC) tienen contraseñas.	X	
Los equipos informáticos están en buen estado.	X	
Los terminales(PC), cuentan con antivirus	X	
Los equipos informáticos están conectados a UPS.		X
Cuentan con un protocolo de seguridad para la protección de los equipos informáticos		X

MATRIZ DE CONSISTENCIA

TITULO	PROBLEMA	OBJETIVO	HIPOTESIS	VARIABLE	TIPO DE DISEÑO DE INVESTIGACIÓN	POBLACIÓN Y MUESTRA
		GENERAL		**UNICA**	**TIPO DE INVESTIGACIÓN**	**POBLACIÓN**
Análisis de Seguridad Informática de los activos en la Institución educativa secundaria Politécnico "Pedro Abel Labarthe Durand", Chiclayo 2019	¿de qué manera un análisis de Seguridad de informática permite identificar vulnerabilidades en los activos de la institución educativa "Pedro Abel Labarthe Durand"?	Analizar la Seguridad Informática de los activos en la Institución educativa secundaria Politécnico "Pedro Abel Labarthe Durand", Chiclayo 2019 **ESPECIFICOS** (1) Conocer la situación actual de la seguridad informática dentro de la Institución educativa "Pedro Abel Labarthe Durand", (2) Identificar los factores de riesgos de los activos de la Institución educativa "Pedro Abel Labarthe Durand" .	Por ser tipo de investigación descriptiva la hipótesis es opcional	Seguridad Informática	APLICADA NO EXPERIMENTAL	La población y la muestra estarán conformada 3 colaboradores de la I.E Pedro Abel Labarthe Durand.

VALIDACIÓN DEL INSTRUMENTO

CUESTIONARIO ENCUESTA – COLABORADORES

ANALISIS DE SEGURIDAD INFORMATICA DE LOS ACTIVOS EN LA INSTITUCION EDUCATIVA SECUNDARIA POLITECNICO "PEDRO ABEL LABARTHE DURAND", CHICLAYO 2019

Responsable: Pedraza Alburquerque Elmer Gabriel

Indicación: Señor(a) especializado(a) le pido su colaboración para que luego de un riguroso análisis de los ítems del cuestionario de la encuesta, que le mostramos marque con un aspa en el casillero que cree conveniente de acuerdo a su criterio y experiencia profesional demostrando si cuenta o no cuenta con los requisitos mínimos de formulación para su posterior aplicación.

NOTA: Para cada pregunta se considera un puntaje del 1 al 5:

1. Insatisfecho	2. Mejorable	3. Satisfecho	4. Bueno	5. Excelente

Nº	ITEMS	Puntaje				
		1	2	3	4	5
1	Existen revisiones periódicas de Hardware y Software					X
2	A su criterio, ¿Qué son normas o procedimientos legales para la seguridad de la información?				X	
3	Conoce Ud. ¿Si existen políticas de seguridad para la información en el centro de sistemas de la información (CSI) de la UGEL?					X
4	A su criterio. ¿Qué existe un personal encargado en atender y rectificar los incidentes ocasionados por las amenazas de la seguridad de información?				X	
5	¿La información que usted utiliza, se encuentra protegida?					X
6	¿La Seguridad al respecto al software, se encuentra protegida?				X	
7	¿Está de acuerdo que se aprueben medidas de seguridad en la UGEL, respalda la información de sus áreas?				X	
8	Según Ud. ¿Se deberia monitorear y evaluar los procesos de contingencia y restauración implementados en la UGEL?					X
9	Alguna vez se le hizo la entrega de algún tipo de documento o plan de seguridad de la información?					X

10	¿Se mantiene programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otro equipo?					X

Recomendaciones:

Mejorar redacción antes de aplicar.

Apellidos y nombres	Cuneo Urbaez Jorge Tomás
Titulo y/o grado académico	Ing. Industrial y de Sistemas.

FIRMA

VALIDACIÓN DEL INSTRUMENTO

CUESTIONARIO ENCUESTA – COLABORADORES

ANALISIS DE SEGURIDAD INFORMATICA DE LOS ACTIVOS EN LA INSTITUCION EDUCATIVA SECUNDARIA POLITECNICO "PEDRO ABEL LABARTHE DURAND", CHICLAYO 2019

Responsable: Pedraza Alburquerque Elmer Gabriel

Indicación: Señor(a) especializado(a) le pido su colaboración para que luego de un riguroso análisis de los ítems del cuestionario de la encuesta, que le mostramos marque con un aspa en el casillero que cree conveniente de acuerdo a su criterio y experiencia profesional demostrando si cuenta o no cuenta con los requisitos mínimos de formulación para su posterior aplicación.

NOTA: Para cada pregunta se considera un puntaje del 1 al 5:

1. Insatisfecho	2. Mejorable	3. Satisfecho	4. Bueno	5. Excelente

Nº	ITEMS	Puntaje				
		1	2	3	4	5
1	Existen revisiones periódicas de Hardware y Software				✓	
2	A su criterio, ¿Qué son normas o procedimientos legales para la seguridad de la información?				✓	
3	Conoce Ud. ¿Si existen políticas de seguridad para la información en el centro de sistemas de la información (CSI) de la UGEL?				✓	
4	A su criterio. ¿Qué existe un personal encargado en atender y rectificar los incidentes ocasionados por las amenazas de la seguridad de información?				✓	
5	¿La información que usted utiliza, se encuentra protegida?					✓
6	¿La Seguridad al respecto al software, se encuentra protegida?				✓	
7	¿Está de acuerdo que se aprueben medidas de seguridad en la UGEL, respalda la información de sus áreas?				✓	
8	Según Ud. ¿Se debería monitorear y evaluar los procesos de contingencia y restauración implementados en la UGEL?				✓	
9	Alguna vez se le hizo la entrega de algún tipo de documento o plan de seguridad de la información?				✓	

10	¿Se mantiene programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otro equipo?				✓	

Recomendaciones:

Apellidos y nombres	NAVARRETE ENRIQUE JONTAS
Titulo y/o grado académico	INGENIERO DE SISTEMAS Y COMPUTACION Mg. EN ADMINISTRACION Y GERENCIA DE EMPRESAS

FIRMA