UNIVERSIDAD PERUANA LOS ANDES

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TESIS:

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA MEJORAR LA SEGURIDAD INFORMÁTICA DE LA I.E. FRANCISCO DE ZELA – HUANCAYO - 2024

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS Y COMPUTACIÓN

Autor: Bach. Kevin Rolando Mateo Condor

Asesores: Mg. Arturo Solis Flores

Mtro. Alfredo Hugo Yapias Rojas

Línea de Investigación: Ciencias Empresariales y Gestión de los Recursos

Huancayo – Perú

2024

HOJA DE CONFORMIDAD DE LOS JURADOS

_____

DR. RUBÉN DARÍO TAPIA SILGUERA

PRESIDENTE

_____

DR. EDWARD EDDIE BUSTINZA ZUASNABAR

JURADO 01

_____

MTRA. JESSICA VILCHEZ GUTARRA

JURADO 02

_____

MTRA. CAROL JOSEFINA FABIAN CORONEL

JURADO 03

_____

MG. LEONEL UNTIVEROS PEÑALOZA

SECRETARIO

DEDICATORIA:

Me complace dedicar esta tesis a mis padres Rolando Mateo Loyola y Mireya Nancy Cóndor Barrera, por su exhortación a seguir mis objetivos a pesar de las dificultades. Quienes con sus enseñanzas hicieron de mí, una persona de bien para la sociedad.

A mi hermana por siempre orientarme con su ejemplo de valentía, perseverancia y sobre todo su gran actitud positiva.

AGRADECIMIENTO:

Agradezco de manera especial a mis asesores los Ingenieros: Alfredo Yapias y Arturo Solis, por el apoyo incondicional, por sus sugerencias para llevar a cabo y hacer todo lo posible para que esta tesis contribuya a nuestra comunidad.

CONSTANCIA DE SIMILITUD

N ° 0226 - FI -2024

La Oficina de Propiedad Intelectual y Publicaciones, hace constar mediante la presente, que la Tesis; titulada:

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA MEJORAR LA SEGURIDAD INFORMÁTICA DE LA I.E. FRANCISCO DE ZELA - HUANCAYO - 2024

Con la siguiente información:

Con Autor(es)	: **Bach. MATEO CONDOR KEVIN ROLANDO**
Facultad	: **INGENIERÍA**
Escuela Académica	: **INGENIERÍA DE SISTEMAS Y COMPUTACIÓN**
Asesor(a) Metodológico	: **Mg. SOLIS FLORES ARTURO**
Asesor(a) Tematico	: **Mtro. YAPIAS ROJAS ALFREDO HUGO**

Fue analizado con fecha 21/06/2024; con 257 págs.; con el software de prevención de plagio (Turnitin); y con la siguiente configuración:

Excluye Bibliografía.	
Excluye citas.	X
Excluye Cadenas hasta 20 palabras.	X
Otro criterio (especificar)	

El documento presenta un porcentaje de similitud de 13 %.

En tal sentido, de acuerdo a los criterios de porcentajes establecidos en el artículo N°15 del Reglamento de uso de Software de Prevención de Plagio Versión 2.0. Se declara, que el trabajo de investigación: ***Si contiene un porcentaje aceptable de similitud.***

Observaciones:

En señal de conformidad y verificación se firma y sella la presente constancia.

Universidad Peruana Los Andes · Oficina de Propiedad Intelectual y Publicaciones · HUANCAYO

Huancayo, 24 de junio del 2024.

MTRA. LIZET DORIELA MANTARI MINCAMI
JEFA
Oficina de Propiedad Intelectual y Publicaciones

CONTENIDO

CONTENIDO DE TABLAS

CONTENIDO DE FIGURAS

RESUMEN

El presente proyecto de investigación titulado: “Sistema de Gestión de la Seguridad de la Información para mejorar la seguridad informática del colegio Francisco de Zela”, surge con la necesidad de resolver los problemas de seguridad de información que se presentan dentro de la Institución Educativa, de tal manera que los riesgos asociados a los activos que tiene la Institución queden menos expuestos a las amenazas y vulnerabilidades que abundan hoy en día; como pregunta general a la formulación del problema se propuso: ¿En qué medida el sistema de gestión de la seguridad de la información favorece la seguridad informática del colegio Francisco de Zela?, para esto la tesis tiene como objetivo, determinar en qué medida el sistema de gestión de la seguridad de la información favorece la seguridad informática del colegio Francisco de Zela, llegando a la hipótesis que el sistema de gestión de la seguridad de la información favorece significativamente la seguridad informática del colegio Francisco de Zela-

Para desarrollar la investigación se usó la metodología propuesta en la ISO/IEC 27001:2022 basados en la gestión de riesgos, los controles y mejoras asociados a ellos, el tipo de investigación utilizado será la investigación Aplicada, el nivel de tipo explicativo y diseño de tipo pre experimental; la población de la investigación está asociada a la comunidad educativa del colegio y la muestra será tomada de los actores principales los cuales son: Docentes, personal administrativo, jerárquico y estudiantes de un grado y sección. Las principales técnicas usadas serán la observación directa y la entrevista teniendo como principal instrumento de recopilación de datos una ficha técnica de registros.

Palabras clave: Sistema de Gestión de la Seguridad de la Información, Seguridad Informática, ISO/IEC 27000:2022, Institución Educativa.

ABSTRACT

The present research project entitled: “Information Security Management System to improve the information security of Francisco de Zela School”, arises with the need to solve the information security problems that occur within the Educational Institution, so that the risks associated with the assets that the Institution has are less exposed to threats and vulnerabilities that abound today; as a general question to the formulation of the problem it was proposed: To what extent the information security management system favors the information security of Francisco de Zela School? The objective of the thesis is to determine to what extent the information security management system favors the information security of the Francisco de Zela school, reaching the hypothesis that the information security management system significantly favors the information security of the Francisco de Zela school.

To develop the research we used the methodology proposed in ISO/IEC 27001:2022 based on risk management, controls and improvements associated with them, the type of research used will be Applied research, the level of explanatory type and pre-experimental design type; the research population is associated with the educational community of the school and the sample will be taken from the main actors which are: Teachers, administrative staff, hierarchical and students of a grade and section. The main techniques used will be direct observation and interview having as main instrument of data collection a technical record sheet.

Key words: Information Security Management System, Information Security, ISO/IEC 27000:2022, Educational Institution.

INTRODUCCIÓN

El presente proyecto de tesis busca analizar el contexto actual en el que la seguridad de información se encuentra, en conjunto con el objetivo general, objetivos específicos y los resultados esperados que se tendrían con la finalización del mismo. Asimismo, se determinará el alcance y las limitaciones que el Sistema de Gestión de Seguridad de la Información tendrá dentro de la institución educativa “Francisco de Zela”, surgidos de la necesidad de resolver los problemas de seguridad de información que se presentan, entre los cuales están: la falta de conciencia sobre seguridad cibernética, infraestructura tecnológica obsoleta, escasa inversión en medidas de seguridad, débil gestión de contraseñas y falta de políticas y protocolos de seguridad claros.

Al plantearse el problema: ¿En qué medida el sistema de gestión de la seguridad de la información favorece la seguridad informática de la I.E. Francisco de Zela?, surge como respuesta la hipótesis: El sistema de gestión de la seguridad de la información favorece significativamente la seguridad informática de la I.E. Francisco de Zela, el cual cumple con el objetivo que fue Determinar en qué medida el sistema de gestión de la seguridad de la información favorece la seguridad informática de la I.E. Francisco de Zela

Para ello, la metodología planteada en la ISO 27001: 2022 basada en la gestión de riesgos, controles y mejoras asociados, servirá como guía para el desarrollo de proyecto. El tipo de investigación será aplicada, con un nivel de tipo explicativo y diseño de tipo pre experimental; obteniendo como muestra a los docentes, personal administrativo, jerárquico y estudiantes de un grado y sección, los cuales conforman parte de la comunidad educativa de la institución. Las principales técnicas usadas serán la observación directa y la entrevista teniendo como principales instrumentos de recopilación de datos una ficha técnica de registros y encuestas.

El Capítulo 1 del trabajo de investigación se presenta comenzando por el planteamiento del problema, describiendo la realidad problemática, los límites, el objetivo, la importancia y el alcance del problema.

El Capítulo 2 brinda el fundamento teórico científico, los contextos nacionales e internacionales, el marco teórico del contexto de la investigación, la definición de los términos clave, el sistema hipotético y las variables que ayudan a comprender el desarrollo global del proyecto de investigación.

El Capítulo 3 muestra las hipótesis de la investigación, en el que también se especifica la noción y el funcionamiento de las variables de la investigación, se señalan los aspectos que deben abordarse y se sugieren los indicadores que deben medirse.

El capítulo 4 presenta la metodología de la investigación en detalle e incluye temas como el tipo, el diseño, la población y la muestra, además de procedimientos generales y particulares, estrategias de recogida y tratamiento de datos, selección de instrumentos y validación de instrumentos.

El capítulo 5 cubre la administración de la planificación, donde se aborda los presupuestos y calendarios.

Finalmente tenemos los anexos con las matrices: de consistencia, operacionalización de variables, operacionalización del instrumento; el instrumento de investigación y el consentimiento informado.

El autor.

I. PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la Realidad Problemática

El mundo en su totalidad a logrado tener un avance significativo en las ciencias de la computación, tecnología digital y sistemas informáticos, implicando así el crecimiento de casos y sofisticación de ataques cibernéticos [1]. A nivel global, cada segundo se detecta millones de ataques, siendo uno de los más fuertes el Spam con 9,846 847 de detecciones por segundo, así lo podemos apreciar en la siguiente imagen, donde el Kaspersky Anti-Spam (KAS) nos brinda las cifras exactas:

Fig. 1. Mapa de tiempo real de amenazas cibernéticas Kaspersky [2]

Latinoamérica no es la excepción al caso, el Panorama de Amenazas en América Latina 2021 de Kaspersky, el equipo de análisis e investigación de Kaspersky realizó un informe anual, revelando un aumento del 24% en ciberataques en nuestro continente en los ocho meses

iniciantes del año, en comparación con el periodo anual anterior [3]. Ahora si fijamos la mirada a nuestro país, en la actualidad, somos uno de los protagonistas en estos eventos, considerados según Kaspersky el país que ocupa el puesto N°22 a nivel mundial en ataques cibernéticos, esto queda evidenciado en el reporte de tiempo real de amenazas elaborados por Kaspersky:

Fig. 2. Mapa de tiempo real de amenazas cibernéticas en Perú [2]

Teniendo en cuenta estos detalles, se observa que la información se ha convertido hoy en día uno de los activos más importante de cualquier organización. Según: [4] Tanto las personas, como la información son los activos más importantes que tiene cualquier organización. La falta de controles y políticas centrados en la seguridad puede tener un impacto significativo en el logro de los objetivos organizacionales o provocar pérdidas más graves de las que la organización anticipó. La creciente dependencia de la tecnología en las organizaciones no sólo beneficia a las empresas, pueden tener efectos potencialmente perjudiciales si no se toman precauciones de ciberseguridad y no se controlan los riesgos en la infraestructura informática y las operaciones corporativas., las empresas están expuestas a una variedad de amenazas y potencialmente a riesgos si se explotan, sus activos de información están en grave riesgo [5]. Esto aplica también para las instituciones educativas, que no quedan exentas a cumplir con controles y políticas adecuadas a sus requerimientos, sin embargo, hoy en día esto aun no queda demostrado en los hechos pues la mayoría de Instituciones educativas, en principal las que están inmersas en el sector público, dejan de lado este tema. No se presta suficiente atención a la seguridad de la información dentro de las instituciones educativas, desde la dirección hasta el propio departamento de TI. [4].

La Institución Educativa “Francisco de Zela” suele realizar sus procesos de manera tradicional sin tomar en cuenta los factores de seguridad requeridos en la actualidad, esto va quedando evidenciado conforme avanza el tiempo pues la mayoría de equipos con los que cuenta la Institución son del año 2013 quedando obsoletos para la realidad actual, en el siguiente diagrama podemos verificar la relación de equipos tecnológicos con la fecha de creación de cada uno de ellos:

TABLA I RELACIÓN DE LOS EQUIPOS TECNOLÓGICOS

TIPO DE EQUIPO	CANTIDAD	AÑO DE FABRICACIÓN
Laptop	92	2013
Impresora	2	2015
Foto copiadora	1	2016
Proyector	11	2013
Cámara de vigilancia	6	2015

Nota: Descripción de los tipos de equipos que maneja la institución, cantidad y año de fabricación.

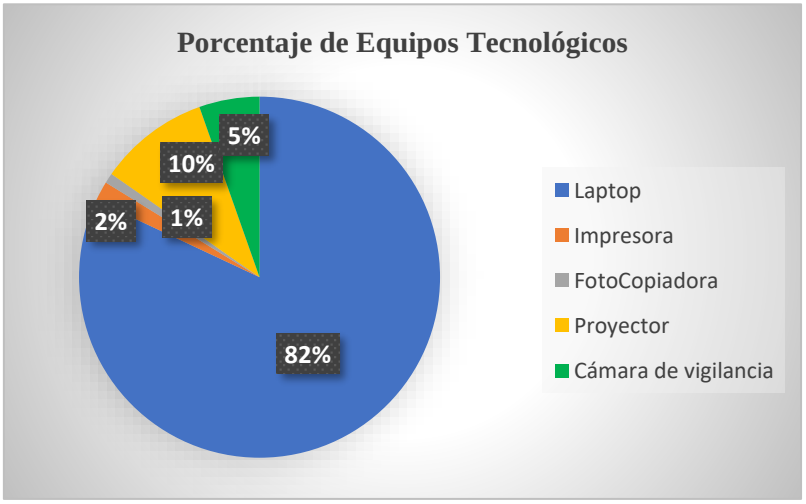

Fig. 3. Gráfico circular de porcentaje de equipos tecnológicos.

En este gráfico queda evidenciado que el 82% de equipos tecnológicos (Laptops) con los que cuenta la Institución Educativa Francisco de Zela tienen como fecha de fabricación el año 2013, esto advierte que son equipos con más de 10 años de antigüedad, los cuales son demasiados antiguos para la realidad actual. Según [6], el tiempo de vida útil de un equipo varia de 3 a 5 años, de ahí para adelante los problemas que se presentarán serán diversos; desde la no actualización de sistema operativo, recalentamiento de las baterías, problemas de compatibilidad con software modernos, etc.; todo esto provocando sistemas operativos desactualizados e interrupción en el servicio educativo.

Por otro lado, la falta de una política clara de seguridad de información hace que el factor humano maneje información sensible de manera confusa creando un grave riesgo de filtración de datos confidenciales, esto queda demostrado después de realizar una encuesta a los usuarios más habituales de los equipos tecnológicos, cuyo porcentaje de desconocimiento se muestra en el siguiente diagrama:

Fig. 4. Gráfico circular de porcentaje de conocimiento de políticas de seguridad de información.

La respuesta a la pregunta: ¿Existe una política de seguridad de información en la Institución?, muestra que el 77% de los usuarios desconoce la existencia de alguna política de seguridad de información dentro de la Institución Educativa, mientras que un 18% asegura si conocer de la existencia del mismo, aclarando que dicha política se encuentra inmersa dentro del RIN (Reglamento Interno) que maneja la Institución Educativa, lo cual no es del todo cierto pues dicho documento se centra en el tema de funciones de cada participante de la comunidad educativa y no en políticas de seguridad de información. Finalmente, existe un 5% de usuarios que no saben o no opinan respecto al tema.

También, la falta de conciencia sobre ciberseguridad, la débil gestión de contraseñas y accesos hace que los activos de información queden vulnerables ante ataques de malware y robo de información. En otras encuestas realizadas a los usuarios de los equipos tecnológicos donde se les consulta respecto a: ¿El nivel de seguridad de los equipos es óptimo para operar en la Institución?, ¿Existe una política de control de accesos establecida y en constante monitoreo? Y ¿Se realiza capacitaciones a todo el personal sobre temas de seguridad de información?, las estadísticas se muestran en los siguientes gráficos:

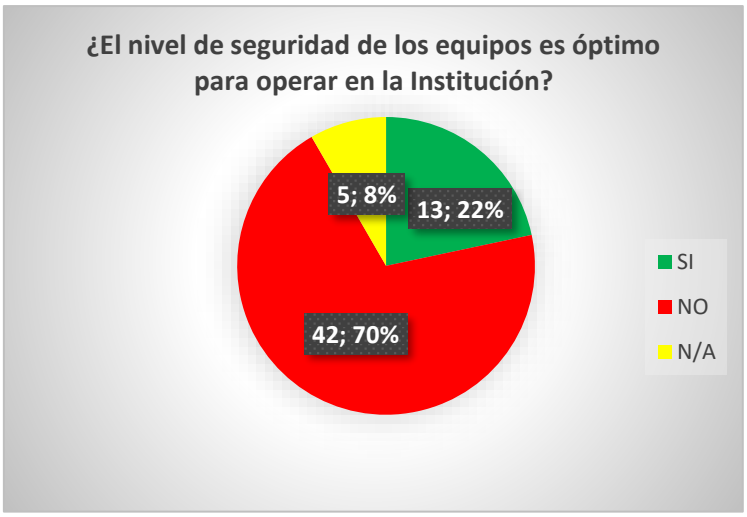

Fig. 5. Gráfico circular de nivel de seguridad.

La figura 5 nos muestra las respuestas de los usuarios a la pregunta: ¿El nivel de seguridad de los equipos es óptimo para operar en la Institución?, quedando en evidencia que el 70% de encuestados creen que el nivel de seguridad de los equipos es poco óptimo para operar en la Institución Educativa, el 22% creen que si es óptimo y el 8% no sabe o no opina respecto al tema.

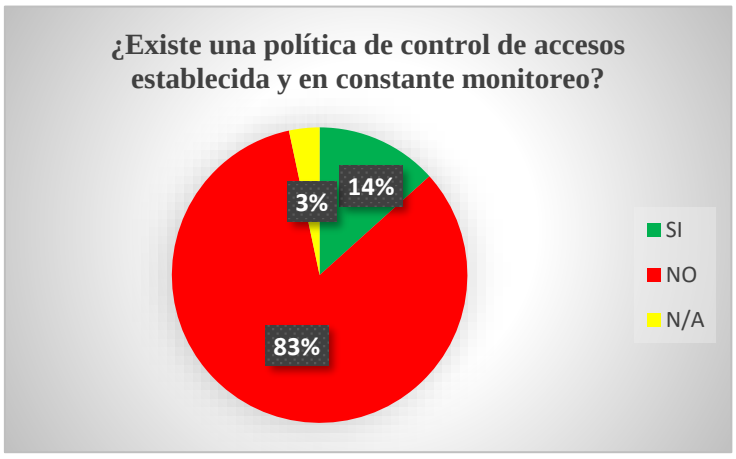

Fig. 6. Gráfico circular de control de accesos.

La figura 6 nos muestra el porcentaje altísimo de negación a la pregunta: ¿Existe una política de control de accesos establecida y en constante monitoreo?, un 83% niega la existencia de una política de control de accesos, mientras que un 14% afirma que sí y un 3% se mantiene al margen de la pregunta.

Fig. 7. Gráfico circular de capacitaciones sobre seguridad de información.

La figura 7 muestra algo más alarmante, sucede que al realizar la última pregunta respecto a si se realizan capacitaciones a todo el personal sobre temas de seguridad de información, el 100% de encuestados afirma no haber recibido ningún tipo de capacitación respecto al tema, lo cual genera un aumento de vulnerabilidades ante amenazas y perdida de datos.

Para finalizar, se muestra un cuadro resumen de todo lo anterior mencionado con el fin de dar a conocer de manera más concisa las causas y efectos producidos dentro de la Institución Educativa:

TABLA II CAUSAS Y EFECTOS DE LA PROBLEMÁTICA

Causas	Problema	Efectos
• Falta de conciencia sobre seguridad cibernética	Escasa seguridad de la información en la Institución Educativa	• Vulnerabilidad ante ataques de malware y robo de información.
• Infraestructura tecnológica obsoleta. Computadoras y Laptops del año 2013		• Sistemas desactualizados y poco seguros, interrupción en el servicio educativo.
• Escasa inversión en medidas de seguridad. Recursos invertidos en otras áreas		• Aumento de vulnerabilidades ante amenazas y pérdida de datos.
• Débil gestión de contraseñas y accesos.		• Riesgo de filtración de datos confidenciales
• Falta de políticas y protocolos de seguridad claros. La institución no cuenta con políticas de seguridad		• Confusión en el manejo de información sensible.

Nota: Descripción de las principales causas y efectos a la problemática.

1.2. Delimitación del Problema

1.2.1. Delimitación espacial

La presente investigación estará centrada en la Institución Educativa “Francisco de Zela”, ubicada en la Región Junín, Provincia de Huancayo, Distrito de El tambo.

1.2.2. Delimitación económica

El plan de tesis se realizó con recursos propios del investigador

1.2.3. Delimitación temporal

El trabajo de investigación comienza el mes de diciembre de 2023, basando los indicadores y requerimientos acorde a la realidad de la Institución Educativa.

1.3. Formulación del Problema

1.3.1. Problema general

- ¿En qué medida el sistema de gestión de la seguridad de la información favorece la seguridad informática de la I.E. Francisco de Zela?

1.3.2. Problemas específicos

- ¿En qué medida el sistema de gestión de la seguridad de la información favorece la seguridad de la información de la I.E. Francisco de Zela?
- ¿En qué medida el sistema de gestión de la seguridad de la información favorece la gestión de riesgos de la información de la I.E. Francisco de Zela?
- ¿En qué medida el sistema de gestión de la seguridad de la información favorece el control informático de la I.E. Francisco de Zela?

1.4. Justificación

1.4.1. Social

Diseñar e implementar un Sistema de Gestión de Seguridad de la Información va a crear un entorno institucional más seguro, haciendo posible que se incremente la reputación y solidez de la Institución Educativa frente a sus competidores a nivel externo y se genere un ambiente de confianza entre la Comunidad Educativa a nivel interno, fomentando un ambiente laboral de mayor confianza.

1.4.2. Teórica

El punto de partida para elaborar un Sistema de Gestión de Seguridad de la Información adecuado a los estándares nacionales e internacionales se basa tanto, en investigaciones

académicas como en teorías plantadas por expertos. La investigación realizada plantea que la toma de decisiones de la Institución Educativa ahora base sus fuentes en el SGSI para que la inversión en seguridad sea aceptada por toda la organización. Por ello, la implementación de los diversos controles nos va a permitir proteger los activos de la Institución Educativa frente a amenazas y riesgos que pongan en peligro la continuidad del servicio educativo.

1.4.3. Metodológica

La presente investigación tiene como objetivo la gestión de riesgos de todos los activos de información de la Institución Educativa con el fin de mitigar las amenazas, identificar las vulnerabilidades y reconocer los requisitos legales asociados. Para ello, la investigación se basa en la ISO/IEC 27001:2022, por lo tanto, la metodología a utilizar irá acorde con la norma con el fin de garantizar un trabajo eficiente y que pueda ser utilizado como referencia aplicable a futuras investigaciones.

1.5. Objetivos

1.5.1. Objetivo general

- Determinar en qué medida el sistema de gestión de la seguridad de la información favorece la seguridad informática de la I.E. Francisco de Zela.

1.5.2. Objetivos específicos

- Determinar en qué medida el sistema de gestión de la seguridad de la información favorece la seguridad de información de la I.E. Francisco de Zela.
- Determinar en qué medida el sistema de gestión de la seguridad de la información favorece la gestión de riesgos de la información de la I.E. Francisco de Zela.
- Determinar en qué medida el sistema de gestión de la seguridad de la información favorece el control informático de la I.E. Francisco de Zela.

II. MARCO TEÓRICO

2.1. Antecedentes

2.1.1. Antecedentes nacionales

- [7] , sustentó la tesis: "Sistema de gestión de seguridad de la información para la calidad de procesos en la I.E.P. Albert Einstein" el año 2023, a la escuela profesional de Ingeniería de Sistemas de la Universidad Nacional de Ucayali, para optar el título profesional de Ingeniero de Sistemas, donde menciona: El objetivo del desarrollo de un sistema de gestión de la seguridad de la información en la calidad de procesos es reducir los riesgos, vulneraciones y sobre todo las amenazas que puedan afectar los activos de información de la agencia y brindar garantías con respecto a la confidencialidad, integridad y disponibilidad de la información de la agencia. Para lograrlo, adoptó el modelo "Planificar – Hacer – Verificar – Actuar", también conocido como PDCA, y lo aplicó en toda la estructura de los procesos. Los resultados muestran que la seguridad de la información y los recursos de información propuestos en el I.E.P. Albert Einstein obtiene un 60% de mejora. Reduce los índices de pérdida de información en diversas áreas gerenciales de la institución a través de recomendaciones para la implementación de sistemas de gestión de seguridad de la información y capacitación continua del personal gerencial en temas de seguridad de la información.

- [8], sustentaron la tesis: "Diseño de un sistema de gestión de la seguridad de la Información basado en la norma técnica peruana -ISO/IEC 27001:2014 para la municipalidad distrital de Huácar 2022" el año 2022, a la escuela profesional de ingeniería de sistemas, para optar el título profesional de ingeniero de sistemas, donde menciona: El proyecto descrito en este documento se basa en el tema de la municipalidad distrital de

Huácar relacionado con los requisitos para la implementación de la norma técnica peruana NTP-ISO/IEC 27001: 2014 en las instituciones nacionales. Para proceder, es necesario realizar una evaluación de esta entidad, desarrollar un sistema de gestión de seguridad de la información (SGSI) para evaluar la seguridad del sistema y cuantificar los activos más valiosos y sus características, reducir o eliminar riesgos y aumentar la productividad y eficacia durante la implementación. Para el desarrollo del SGSI utilizamos la versión 3 de Análisis y Gestión de Riesgos de Sistemas de Información - Metodología MAGERIT para el análisis de activos y la gestión de riesgos. Comience analizando la evaluación del estado inicial de su organización para planificar y diseñar su SGSI. Con base en el análisis de activos definido en MAGERIT V3, iniciar el procesamiento de riesgos y proceder a refinar e implementar controles de seguridad relacionados con el diseño NTP - ISO/IEC 27001: 2014. Elaborar una declaración de solicitud de acuerdo con las pautas y proponer una política de seguridad de la información adaptada a la situación del municipio del distrito de Huácar. Los resultados muestran una falta de seguridad de la información en la comunidad. Por tanto, la documentación proporcionada utiliza los controles más adecuados para su posterior implementación en este área y proceso del SGSI.

- [9], sustentó la tesis: "Sistema de gestión de seguridad de la información para mejorar la protección informática de la Comisaria Región Huancavelica" el año 2019, a la escuela de formación profesional de Ingeniería de Sistemas y computación de la Universidad Nacional Daniel Alcides Carrión, para optar el título profesional de Ingeniero de Sistemas, donde menciona: Este estudio tiene como objetivo evaluar y analizar los factores de riesgo que surgen dentro de una institución, proteger sus datos e información valiosa con la ayuda de sistemas de gestión de seguridad de la información, identificar, gestionar y minimizar los riesgos que pueden amenazar la seguridad de la información. Es importante distinguir entre seguridad informática y seguridad de la información. Primero, la seguridad informática se refiere a proteger la infraestructura de tecnología de la información y las comunicaciones que respalda nuestro negocio. Ejemplos de información que se puede encontrar dentro de nuestra organización incluyen correos electrónicos, páginas web, imágenes, bases de datos, faxes, contratos, presentaciones, documentos, etc. Además, se debe considerar el ciclo de vida de la información. Esta metodología permite, en primer lugar, analizar y organizar la estructura de los sistemas de información. En segundo lugar, es más fácil definir flujos de trabajo para garantizar la seguridad. La gestión de riesgos a través de sistemas de gestión de seguridad de la información nos permite mantener la

confidencialidad, integridad y disponibilidad interna de nuestros clientes y diversos stakeholders internos.

- [10], sustentó la tesis: "Diseño de un sistema de gestión de seguridad de la información para la Corte Superior de Justicia de Piura, mediante la normativa ISO/IEC 27001" el año 2020, a la escuela profesional de Ingeniería de Sistemas de la Universidad César Vallejo, para optar el título profesional de Ingeniería de Sistemas, donde menciona: El objetivo general del estudio es el sistema de gestión de seguridad de la información de la Corte Suprema de Piura basado en la norma ISO/IEC 27001. Mediante el diseño y aplicación no experimental de las fases del Modelo de Aplicación de Deming (PDCA), se utilizaron las fases de "planificar, hacer, controlar y actuar" como dimensiones para la implementación del sistema de gestión de seguridad de la información. Los niveles de cumplimiento y la frecuencia de incidentes detallados para los 114 controles incluidos en la norma ISO 27001 se determinaron utilizando los protocolos existentes de la agencia. Finalmente, los controles para el seguimiento y verificación de la seguridad de la información en la Corte Suprema de Piura se basan en la norma ISO 27001 con sus respectivos indicadores, de acuerdo a las necesidades de las 10 políticas de seguridad más convenientemente determinadas en la brecha de seguridad de la información. en. Se concluye que los riesgos identificados se evalúan con un nivel de severidad medio e incluyen equipos de procesamiento de datos, equipos de comunicación e información en formato digital. Finalmente, se desarrolló un sistema de gestión de seguridad de la información basado en lineamientos con sus respectivos indicadores para la Corte Suprema de Piura a través de la norma ISO/IEC 27001. Gestión de riesgos a través de sistemas de gestión de seguridad La información nos permite mantener la confidencialidad, integridad y disponibilidad de la información internamente, para nuestros clientes y para las diversas partes involucradas en nuestro negocio.

2.1.2. Antecedentes internacionales

- [11], sustentó la tesis: "Análisis y diseño para un modelo de gestión de seguridad de información basados en normas iso/iec27001:2013 para la empresa Artehogar en la ciudad de guayaquil" el año 2019, a la facultad de Ciencias Administrativas de la Universidad de Guayaquil, con la finalidad de optar el grado de Maestría en Ingeniería en Sistemas Administrativos Computarizados, donde menciona: Que luego de un estudio realizado a la empresa se concluye que es de vital importancia la implementación del modelo de gestión

de seguridad de la información ya que permite poner al descubierto vulnerabilidades y nos provee herramientas valiosas para elaborar fuertes procedimientos de seguridad.

Se demostró que la empresa debe estar en constante aseguramiento de sus activos de información, indicando que todo activo así sea el más mínimo debe estar asegurado y cubierto por procedimientos de seguridad, demostrando que una zona que no esté protegida se convierte en una potencial entrada para personas malintencionadas.

- [12], realizaron la tesis: "Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico" el año 2018, a la Facultad de Ingeniería de Sistemas, Universidad Autónoma de Manizales, Manizales, Colombia, llegando a las siguientes conclusiones: Las batallas políticas plantean la posibilidad de que la información institucional se haga pública, especialmente en épocas electorales. Este es un riesgo que podría perjudicar al IED, así como a la información que puedan tener los profesores, el personal administrativo, los niños y los adolescentes.

  Los miembros del personal encargados de mantener, administrar y controlar la información de alumnos, adolescentes y profesores no son conscientes de las consecuencias que surgen cuando se materializan las amenazas a la seguridad de la información.

  El modelo de SGSI constituye una herramienta que genera cultura sobre la disposición de los desechos tecnológicos de las IED's previniendo que las áreas circundantes se vean contaminadas visual y químicamente por el inadecuado manejo de los activos que han sido dados de baja del inventario.

  El concepto de SGSI propuesto contribuye a la sociedad protegiendo la información privada de niños y adolescentes de agentes sospechosos que la utilizarían para reclutarlos en redes de prostitución infantil y pornografía.

- [13],sustentaron la tesis: "Diseño de un modelo de gestión de seguridad de información en el área de talento humano de la secretaría de educación" el año 2017; a la facultad de Ingeniería y Ciencia Básicas de la Institución Universitaria Politécnico Grancolombiano, con la finalidad de optar el grado de especialista en seguridad de la información, donde menciona:

  El diseño por parte de la secretaría de un Sistema de Gestión de la Seguridad de la Información, o SGSI, permite identificar los puntos débiles de la organización y

proporciona herramientas cruciales para crear políticas que apoyen en gran medida la seguridad.

Es importante que todos los involucrados en la organización conozcan los beneficios y ventajas de SGSI, asimismo involucrarlos en los procesos de implantación del plan de seguridad de la información para que vean cómo afecta en sus labores.

2.2. Bases Teóricas o Científicas

2.2.1. Sistema de Gestión de la Seguridad de la Información

[14].Un SGSI es un enfoque sistemático basado en el ciclo PDCA, el cual se basa en establecer, implementar, operar, monitorear, revisar, mantener y realizar la mejora continua de la seguridad de la información de una organización. Basado en utilizar de la manera más efectiva posible una metodología que nos permita tratar y administrar la evaluación de riesgos y en niveles de aceptación de riesgos de la organización. Para contribuir aún más con una implementación exitosa de un SGSI será necesario el análisis adecuado de los requisitos y aplicación de controles apropiados para garantizar la óptima protección de los activos de información.

Optar por un SGSI tiene que ser una decisión estratégica para la organización, su implementación va a estar relacionada a los objetivos, requerimientos de seguridad, los procesos institucionales y nivel de complejidad de la organización. Por ello, una administración adecuada del SGSI mantiene la confidencialidad, integridad y disponibilidad en el manejo y tratamiento de la información [14].

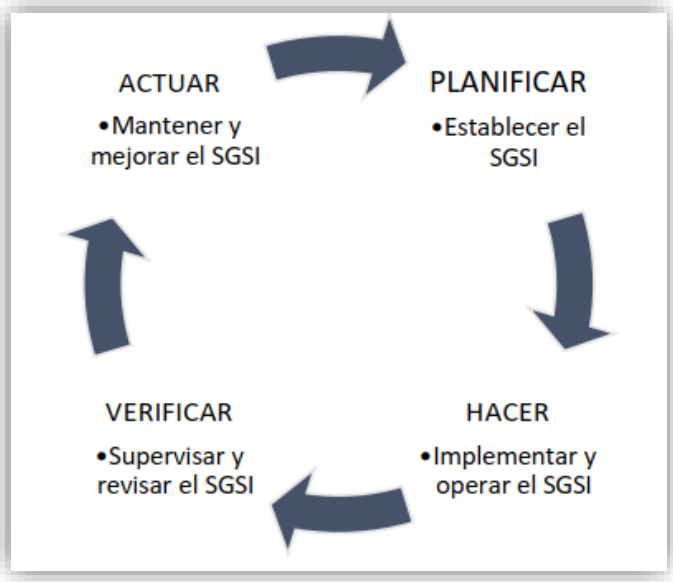

Fig. 8. Ciclo PDCA en la ISO/IEC 27000 [14].

2.2.1.1. Diagnóstico de situación actual

Basado en el análisis de requerimientos de la institución comenzando por la identificación de activos para finalizar con la estimación de los riesgos.

Identificación de Activos

El primer paso para un SGSI será el identificar todos los activos existentes en una organización sin importar el tamaño para tener un punto de partida con una visión clara de los objetivos a lograr, para ello, tenemos que tener en cuenta que un activo es un: "Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos"[15]

Identificación de Amenazas

Como siguiente paso es elaborar un cuadro con las amenazas que puedan ocurrir en la organización. Para ello tenemos que tener en cuenta que una amenaza es una: Potencial causa referida a un incidente, el cual puede causar daños a una institución o a un sistema de información [15].

Identificación de Vulnerabilidades

Según: [16], la vulnerabilidad de un activo es la materialización potencial o gran posibilidad de ocurrencia de una amenaza sobre dicho activo. Las vulnerabilidades nos muestran el nivel de seguridad al cual se encuentra expuesta la organización en nuestro caso referida a la Institución Educativa.

Gestión de riesgos

[16], Selección e implementación de medidas de protección para detectar, prevenir, detener, disminuir o controlar los riesgos identificados. Este paso como uno de los principales para administrar de manera óptima todo lo anterior mencionado y poder tener un control adecuado para la seguridad. La metodología Magerit V3. Es muy utilizada para la gestión de riesgos, si bien es cierto no la utilizaremos como base para el presente proyecto, nos brinda muchas pautas para abordar de manera adecuada este proceso y así mantener un control más ordenado de los riesgos a los que se pone la institución.

2.2.1.2. Implementación de un SGSI.

Continuando con el famoso ciclo de Deming (PDCA), pasaremos a la fase de implementación partiendo por cuatro pilares:

- Crear un plan de respuesta a riesgos.
- Implementar los controles seleccionados.
- Medir la eficacia de estos controles.
- Desarrollar programas de capacitación y sensibilización.

2.2.1.3. Monitoreo y Revisión.

Gestión y evaluación del SGSI, cumplimiento de las políticas, revisiones periódicas de la efectividad del SGSI, teniendo en cuenta los objetivos del SGSI y revisiones de controles de seguridad, resultados de auditorías de seguridad, herramientas de vulnerabilidad, incidentes y resultados. incidentes, resultados.

2.2.2. Seguridad Informática

Según [17] La seguridad informática, cuyas siglas en inglés son IT Security, es un campo encargado de implementar soluciones tecnológicas para proteger la información. "La seguridad informática busca proteger los sistemas informáticos y garantizar la integridad y confidencialidad de la información que contienen". Por lo tanto, mantiene la infraestructura y las comunicaciones que soportan las operaciones de una empresa, el hardware y software que utiliza una empresa. Se puede decir que es la implementación de medidas técnicas [17] .

Las prácticas para este tipo de seguridad varían, pero generalmente consisten en restringir el acceso al sistema o partes del mismo. El acceso se otorga únicamente a personal autorizado específico y se permiten cambios dentro del alcance de su autorización. Las amenazas encontradas se deben a que los propios usuarios no tienen en cuenta las vulnerabilidades existentes a la hora de explotar el sistema. Por ejemplo, descarga archivos peligrosos o elimina archivos importantes del sistema. Al mismo tiempo, pueden aparecer programas maliciosos como virus y malware [18] .

2.2.2.1. Seguridad de la Información.

Es una disciplina que informa sobre riesgos, amenazas, análisis de escenarios, buenas prácticas y sistemas regulatorios, y la necesidad de garantizar el nivel de procesos y tecnologías

que se crean, utilizan, almacenan y son confiables. Transmisión, recuperación y eventual distribución de información [18].

La seguridad de la información tiene como objetivo garantizar la confidencialidad, integridad y disponibilidad de la gestión de la información de los activos mediante la evaluación de riesgos y amenazas, la preparación de planes de acción y la minimización de riesgos de acuerdo con las regulaciones o mejores prácticas, es una disciplina que asume la responsabilidad de adaptarse. La seguridad de la información es una disciplina responsable de garantizar que: - Confidencialidad, - Integridad y - Disponibilidad de la información.

La seguridad de la información suele estar respaldada por políticas de seguridad desarrolladas mediante el desarrollo de un plan maestro de seguridad. La Dirección es responsable de definir todos los cursos de acción relacionados con la seguridad y, a través del Plan director, las medidas tanto técnicas como procedimentales para garantizar que se alcancen los objetivos establecidos en la política de seguridad. Las medidas técnicas son realizadas por equipos de seguridad informática, administradores de sistemas y seguridad, roles de seguridad que implementan las medidas necesarias para cumplir con las políticas de seguridad y el análisis de riesgos que subyace a las políticas [18].

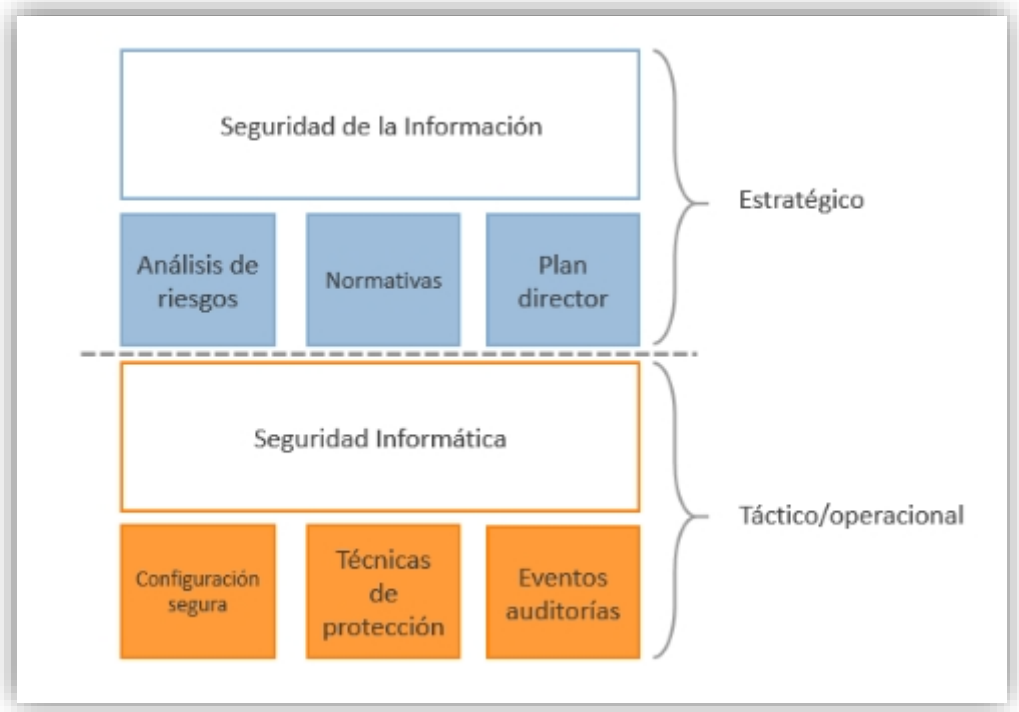

Fig. 9. Comparativa entre Seguridad de Información y Seguridad Informática[17]

2.2.3. ISO/IEC 27000

La norma internacional ISO 27000 es una serie de normas desarrolladas por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. Todos estos estándares proporcionan un marco para la gestión de la seguridad de la información que cualquier organización o empresa puede utilizar [13].

Dos de las normas ISO/IEC 27000 se publican a continuación:

2.2.3.1. ISO/IEC 27001.

Según [14], un Sistema de Gestión de Seguridad de la Información (SGSI) consiste en mantener los pilares que sostiene: disponibilidad, confidencialidad e integridad. Estos representan los fundamentos subyacentes a la seguridad de la información. La confidencialidad requiere que esta información se mantenga fuera del alcance de personas, organizaciones o procesos que no estén autorizados a utilizarla. La integridad consiste en disponer de información completa y precisa. Finalmente, la disponibilidad se refiere a la disponibilidad oportuna de información para las personas, organizaciones o procesos cuando la necesitan.

2.2.3.2. ISO/IEC 27002.

Una ampliación más profunda y explicada de la ISO/IEC 27001 se puede encontrar en esta norma creada a modo de informe. Los primeros principios fueron publicados en los 2000 bajo el antiguo nombre de "ISO 17799", con el título "Tecnología de la Información – Técnicas de seguridad – Código de prácticas para la gestión de la Seguridad de la Información". Ya a mitad del año 2007 fue alineado a la familia de los ISO 27K, con esto las prácticas operacionales se ofrecieron a medida de métodos y procedimientos adaptables a los diferentes requerimientos de las organizaciones [19].

2.3. Marco Conceptual (de las variables y dimensiones)

- **Activo:** "Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos"[15].

- **Amenaza**: "Potencial causa de un incidente no-deseado, el cual puede terminar dañando el sistema"[14].

- **Análisis de riesgos:** "Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización"[16].

- **Ataque:** “Actos deliberados encaminados a vulnerar los mecanismos de seguridad de los sistemas de información”[16].
- **Confidencialidad**: “Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso”[16].
- **Riesgo:** “Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la Organización”[16].
- **Información:** “La información es un conjunto organizado de datos procesados que representa un mensaje que cambia el nivel de conocimiento de la entidad o sistema que recibe el mensaje”[9].
- **Inventario de activos**: “Dentro del alcance de un SGSI, una lista de todos los recursos (recursos físicos, información, software, documentos, servicios, personas, activos intangibles, etc.) que tienen valor para una organización y, por lo tanto, deben protegerse de riesgos potenciales”[14].
- **Informática**: “La ciencia que estudia métodos automáticos y racionales de información mediante la adquisición, transformación, uso y comunicación de información a través de recursos de información computacionales”[15].

III. HIPÓTESIS

3.1. Hipótesis General

- El sistema de gestión de la seguridad de la información favorece significativamente la seguridad informática de la I.E. Francisco de Zela.

3.2. Hipótesis Específicas

- El sistema de gestión de la seguridad de la información favorece significativamente la seguridad de información de la I.E. Francisco de Zela.
- El sistema de gestión de la seguridad de la información favorece significativamente la gestión de riesgos de la información de la I.E. Francisco de Zela.
- El sistema de gestión de la seguridad de la información favorece significativamente el control informático de la I.E. Francisco de Zela.

3.3. Variables

3.3.1. Sistema de Gestión de la Seguridad de la Información

3.3.1.1. Definición conceptual.

"Los elementos interrelacionados o que interactúan (estructura organizacional, políticas, planes de acción, responsabilidades, procesos, un conjunto de procedimientos y recursos). Basados en la Gestión de riesgos y mejora continua"[14].

3.3.1.2. Definición operacional.

"Un SGSI es un enfoque sistemático basado en el ciclo PDCA, el cual se basa en establecer, implementar, operar, monitorear, revisar, mantener y realizar la mejora continua de la seguridad de la información de una organización"[14].

3.3.2. Seguridad Informática

3.3.2.1. Definición conceptual.

"La seguridad informática busca proteger los sistemas informáticos y garantizar la integridad y confidencialidad de la información que contienen”[17]

3.3.2.2. Definición operacional.

La seguridad informática se basa en salvaguardar la seguridad de información, gestionar los riesgos de información y el control informático, contemplando los niveles de seguridad, políticas de gestión, políticas de control de accesos, controles de seguridad, políticas criptográficas, planes de continuidad operativa, etc.

3.3.3. Operacionalización de variables

TABLA III OPERALIZACIÓN DE VARIABLES

Variables	Definición Conceptual	Dimensiones	Indicadores	Ítems	Formula	Instrumento
Variable Independiente: Sistema de Gestión de la Seguridad de la Información	"Los elementos interrelacionados o que interactúan (estructura organizacional, políticas, planes de acción, responsabilidades, procesos, un conjunto de procedimientos y recursos). Basados en la Gestión de riesgos y mejora continua"[14].	Diagnóstico de situación actual	Activos identificados y valorados	Cantidad de activos	% de frecuencia con que se repite	Guía de Observación 1
			Amenazas sobre activos de información	Cantidad de amenazas	% de frecuencia con que se repite	Guía de Observación 2
			Vulnerabilidades sobre activos de información	Cantidad de vulnerabilidades	% de frecuencia con que se repite	Guía de Observación 3
			Estimación del nivel de riesgo	Riesgo bajo, medio, alto	% del total	Guía de Observación 4
		Implementación del SGSI	Controles aplicados según normativa	Políticas de seguridad de información, Seguridad de recursos humanos	Porcentaje de cumplimiento	Lista de control 1
			Tasa de incidencias registradas	Tasa de incidencias registradas	Cantidad de incidencias	Guía de observación 5
		Monitoreo y revisión	Indicadores para procedimientos de monitorización	Nivel de conocimiento de la política de seguridad en colaboradores	Frecuencia de medición semestral	Lista de control 2
Variable dependiente: Seguridad Informática	"La seguridad informática busca proteger los sistemas informáticos y garantizar la integridad y confidencialidad de la información que contienen"[17].	Seguridad de la Información	Nivel de seguridad de equipos	¿El nivel de actualizaciones de seguridad, soluciones antivirus y antimalware son óptimos para trabajar en la institución?	$SI = \frac{R}{T} X100$ Donde: SI: Seguridad de información T: Total de encuestados R: Respuestas	Cuestionario Encuesta Ficha de observación Ficha técnica
			Nivel de políticas de gestión de clases de cifrado	¿Se almacena y gestiona las contraseñas de forma segura?		
			Nivel de políticas de control de acceso	¿Se registran y monitorean intentos de acceso no autorizados?		
			Nivel de segregación de funciones y responsabilidades	¿En qué nivel se encuentran divididas las funciones y responsabilidades a fin de reducir los cambios sin autorización o el uso indebido de información o servicios?		
			Nivel de aseguramiento de controles de seguridad	¿Se tienen políticas de acceso físico y procedimientos		

				establecidos para la gestión de incidentes de seguridad?		
			Nivel de procedimientos para eliminación de accesos	¿En qué escala, existe un procedimiento para garantizar que al término del vínculo laboral los usuarios sean deshabilitados de todos los accesos informáticos?		
		Riesgo de la información	Nivel de aceptación de acuerdos	¿Se realiza un seguimiento de la aceptación y cumplimiento del acuerdo de seguridad por parte de los usuarios?	$RDI = \frac{RRDI}{TRDI} x100$ Donde: RDI: Riesgo de la Información RRDI: Respuestas TRDI: Total de encuestados	
			Nivel de existencia de procedimientos de destrucción	¿Existe un procedimiento para destruir los datos obsoletos o inútiles?		
			Nivel de protección de datos	¿El nivel de seguridad de las copias de respaldo son los óptimos para proteger los datos y documentos contra, destrucción, perdida, falsificación, accesos y divulgación no autorizada?		
			Nivel de planes para la continuidad operativa	¿Se maneja una política de escritorio limpio a fin de evitar divulgación de datos confidenciales?		
		Control informático	Nivel de capacitaciones de seguridad de la información	¿Se proporciona capacitaciones en seguridad de la información a todos los usuarios de los equipos informáticos de la Institución?	$IC = \frac{TIC}{TICD} x100$ Donde: IC: Control informático TIC: Respuestas TCID: Total de encuestados	
			Nivel de concientización de la seguridad de información	¿Se elabora un plan de concientización respecto a temas de seguridad de la información?		

Nota: División de la variable independiente y dependiente con sus respectivas dimensiones e indicadores.

IV. METODOLOGÍA

4.1. Método de Investigación

Se utilizará el método científico como un método general para la presente investigación. Para conocer un poco más sobre que nos aporta un método científico se toma el siguiente concepto: “Un método de procedimiento que ha caracterizado a las ciencias naturales desde el siglo XVII, que consiste en la observación, medición y experimentación sistemáticas, y la formulación, prueba y modificación de hipótesis”[20].

Como método específico se empleará el “método analítico-sintético” ya que partiremos de una descomposición en partes individuales del objeto de estudio y luego integraremos las partes para estudiarlas en su conjunto de manera integral, fomentando así el análisis y síntesis del estudio.

4.2. Tipo de Investigación

El tipo de investigación que se desarrollará es la investigación Aplicada, la cual nos proporcionará la protección de sistemas y aplicativos implementados dentro de la institución educativa, siendo estos de suma importancia para el desarrollo del diseño de un sistema de gestión de la seguridad de la información.

4.3. Nivel de Investigación

El nivel de investigación es de tipo explicativa, la cual nos ayuda a conocer a detalle la profundidad de las causas en las que se ocasiona el problema y el desarrollo real en el cual se produce.

4.4. Diseño de la Investigación

El diseño de investigación es de tipo pre experimental, ya que se aplica como variable independiente al sistema de gestión el cual surtirá un efecto en la seguridad informática (variable dependiente) de la institución ya sea de manera negativa o positiva.

Respecto al diseño de investigación pre experimental. [20], explica que el diseño pre experimental es como una aplicación la cual realiza una prueba previa (pre test) a un grupo o tratamiento experimental, para que después se aplique una medición posterior (post test).

4.5. Población y Muestra

4.5.1. Población

Para [20]: "*Las poblaciones deben situarse claramente por sus características de contenido, lugar y tiempo*" es por ello que la población para el caso de estudio está conformada por toda la comunidad educativa de la Institución Educativa "Francisco de Zela" compuesta de la siguiente forma:

TABLA IV ORGANIGRAMA DE LA INSTITUCIÓN FRANCISCO DE ZELA

TIPO	CARACTERÍSTICA	CANTIDAD
Personal Jerárquico	• Directora • Coordinadores Pedagógicos y de tutoría	4
Personal Administrativo	• Psicólogo • CIST • Personal de Vigilancia y Mantenimiento	6
Docentes	• Docentes por áreas pedagógicas	19
Estudiantes	• Del 1ro al 5to Grado divididos en dos secciones: "A" y "B".	246
	TOTAL	275

Nota Descripción del tipo de personal dentro da la institución educativa y sus principales características.

4.5.2. Muestra

La muestra "es un subgrupo de la población de interés sobre el cual se recolectarán datos, y que tiene que definirse y delimitarse de antemano con precisión, además de que debe ser representativo de la población" [20, p. 173].

Para la investigación nos centramos en: El personal Jerárquico, Personal administrativo, docentes, los cuales suman un total de: **29 personas**.

4.6. Técnicas e Instrumentos de Recopilación de Datos

4.6.1. Técnicas de recopilación de datos

Una de las técnicas más usadas en la presente investigación será: la observación directa para luego poder ser anotado en las fichas técnicas, también se usará la entrevista como otra técnica adicional en el cual se aplicará un cuestionario al personal educativo [20].

4.6.2. Instrumentos de recopilación de datos

La ficha técnica de registros es el instrumento que se utilizará, teniendo una constancia escrita de los sucesos. Las fichas serán de Pre test y Post test [19].

Registro de incidentes, entrevistas, informes de gestión de riesgos serán instrumentos adicionales que también serán aplicados a la investigación.

4.7. Técnicas de Procesamiento y Análisis de Datos

4.7.1. Técnicas de procesamiento

Se utilizará la técnica de procesamiento Batch. Además, se utilizarán las siguientes herramientas: Microsoft Excel y SPSS versión 25.

4.7.2. Análisis de datos

Se utilizará los fundamentos teóricos de la estadística descriptiva, pruebas de medidas y tablas de frecuencias [10].

4.8. Aspectos Éticos de la Investigación

Tanto la seguridad de la información proporcionada por la Institución educativa como la importancia y exactitud de los resultados e identidad de las personas involucradas son asumidos por el investigador. También el examen del marco teórico, citando antecedentes generados por las políticas en archivos y la aplicación de herramientas para ser evaluadas e implementadas [21].

Participación voluntaria: Absolutamente todos los sujetos de investigación son libres de abandonar el presente estudio sin ningún tipo de presión o coacción.[21]

Consentimiento informado: Absolutamente todos los participantes de la investigación recibieron y comprendieron toda la información necesaria para decidir o no participar en la investigación [21].

Anonimato y Confidencialidad: La información recopilada no muestra los datos personales del participante a fin de garantizar el total anonimato de sus respuestas y en caso de ser

necesario sus datos personales, queda estrictamente reservado para la presente investigación sin divulgación a terceras personas [21].

Comunicación de resultados: Los resultados serán los más transparentes posibles, basados en la confiabilidad y credibilidad [21].

V. RESULTADOS

5.1. Descripción del diseño tecnológico

5.1.1. Implementación del SGSI

1. PLANIFICAR

A. CONTEXTO DE LA ORGANIZACIÓN

A.1. ENTENDER LA ORGANIZACIÓN

DATOS GENERALES:

DRE : JUNÍN

UGEL : Huancayo

I.E. : Francisco de Zela

Código Modular : 0919308

Código de Local : 223208

Directora : Lic. Rosario Gavilán Hilario

Año : 2023

Dirección : Calle Rosario 632

Modelo : JEC

MISIÓN

“Somos una institución que empodera a nuestros estudiantes para que afiancen sus aprendizajes establecidos en el CNEB, lleven una vida basada en la integridad personal y creen soluciones socialmente responsables, logrando culminar la escolaridad”[22].

VISIÓN

“Al 2025, la IE Francisco de Zela, se consolida como una I.E. líder e innovadora que responde eficientemente a las necesidades del mundo globalizado, garantizando que sus estudiantes logren la autonomía y el éxito en sus proyectos de vida, con una propuesta de formación integral, que promueva el desarrollo de una ciudadanía activa; a través del a conciencia social con responsabilidad en el cuidado del medio ambiente”[22].

VISIÓN COMPARTIDA

“Ser Zeleño es ser un ejemplo de vida”[22]

VALORES

- Solidaridad planetaria y equidad intergeneracional
- Justicia
- Respeto
- Solidaridad
- Perseverancia
- Responsabilidad
- Tolerancia
- Honestidad
- Equidad
- Responsabilidad Social y Ambiental

ÓRGANOS QUE COMPONEN LA I.E. Y ORGANIGRAMA

ÓRGANO DE DIRECCIÓN:

- Dirección.

ÓRGANO PEDAGÓGICO

- Coordinador de Tutoría
- Coordinadores Pedagógicos (ciencias y letras)
- Coordinador de Innovación y Soporte Tecnológico

ÓRGANO DE EJECUCIÓN

- Personal Docente
- Auxiliar de Educación

ÓRGANO DE SOPORTE AL PROCESO PEDAGÓGICO:

- Psicólogo o trabajadora social.
- Personal de mantenimiento
- Personal de Vigilancia

ÓRGANO DE PARTICIPACIÓN, CONCERTACIÓN Y VIGILANCIA:

- Consejo Educativo Institucional. (CONEI)
- Comité de Recursos Financieros (COREFI)
- Comité de Infraestructura. (COINFRA)
- Comunidad Magisterial
- Municipio Escolar

ÓRGANO DE APOYO:

- Consejo Directivo de APAFA.
- Comités de Aula de Padres de Familia.

ORGANIGRAMA ESTRUCTURAL

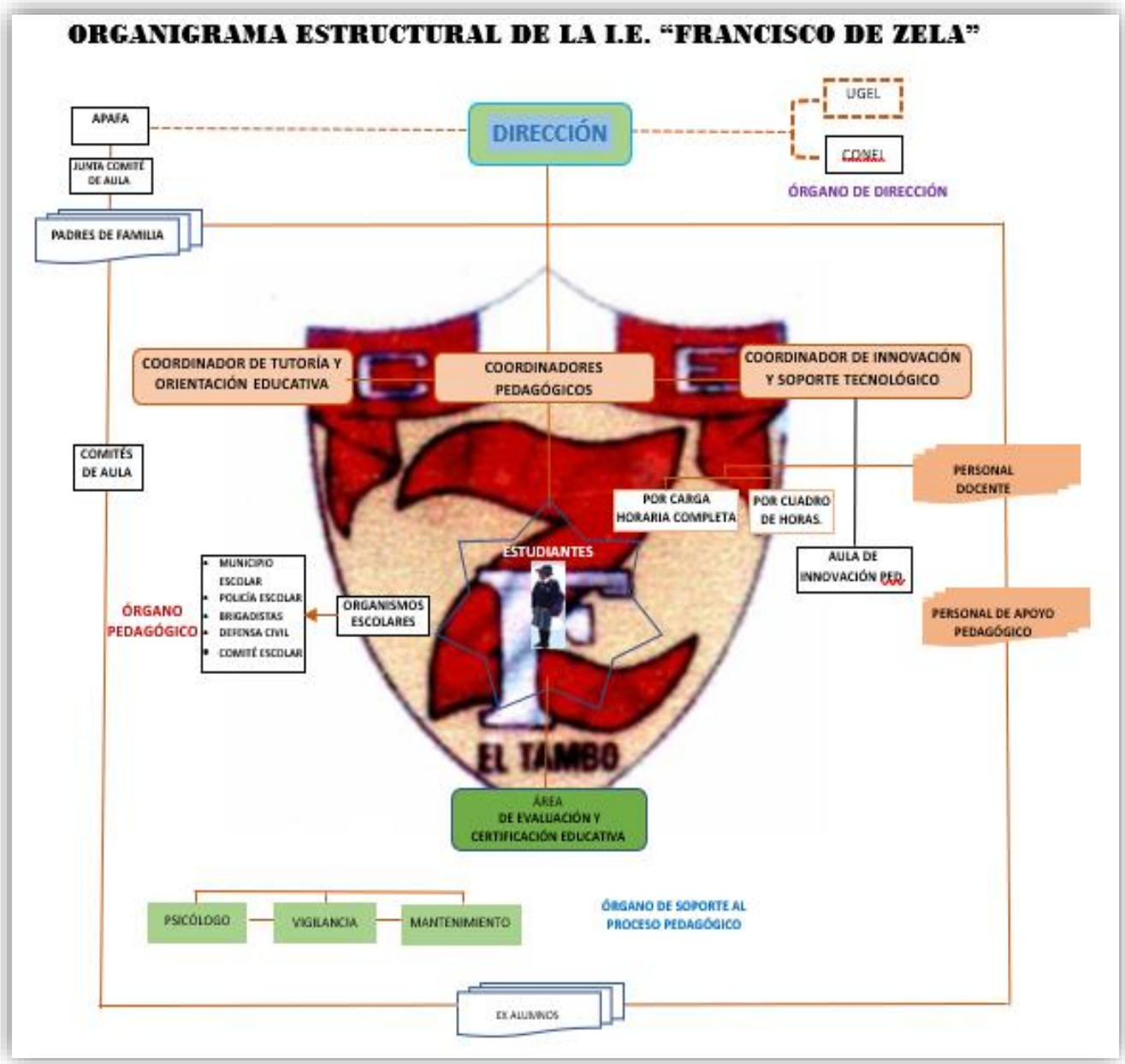

Fig. 10. Organigrama Estructural "Francisco de Zela"

FUNCIONES Y RESPONSABILIDADES

"Las funciones asignadas a los diferentes órganos y sus representantes, consignados en el manual de funciones emitidos por la Dirección Regional de Educación de Junín, en concordancia con la Ley General de Educación N° 28044, Ley N° 29944 "Ley de la Reforma Magisterial y su modificatoria L.D 30541" D.S. N° 004-2013-ED – Reglamento de la Ley N° 29944, y demás normas educativas vigentes aplicables en cuanto alcance al presente reglamento los servidores; tienen las siguientes funciones:"[22]

Responsabilidades del director:

El director actúa como agente legal y máxima autoridad de la institución educativa. Además de las responsabilidades señaladas en los párrafos 55° y 68° de la Ley General de Educación, es responsable de lo siguiente:

a. "Representa legalmente a la institución educativa"[23].

b. "Formula, coordina, ejecuta y evalúa el PEI., PCI., RIN y Plan de Trabajo Anual, conforme a los objetivos educacionales"[23].

c. "Vela por el cumplimiento de los objetivos educacionales y por el buen trato de los alumnos dentro y fuera del colegio"[23].

d. "Preside las reuniones técnico pedagógico, colegiados y GIA, así como las administrativas y otras relacionadas con los fines de la I.E"[23].

e. "Autoriza visitas de estudio de acuerdo a las normas vigentes y específicas"[23].

f. "Matrícula de oficio al menor abandonado o en peligro moral, y pone el caso en conocimiento de las autoridades e instituciones pertinentes"[23].

g. "Autoriza la rectificación de nombres y apellidos de los educandos en los documentos pedagógicos oficiales de acuerdo a normas específicas"[22].

h. "Actualiza y aprueba anualmente el Reglamento Interno"[23].

i. "Dirige, coordina, estimula y evalúa al personal docente, administrativo y de CAS a su cargo"[23].

j. "Organiza y evalúa los servicios de matrícula, exoneración de asignaturas y pruebas de evaluación"[23].

k. "Administra el uso de ambientes, equipos y la documentación de la I.E"[23].

l. "Garantiza el desarrollo gradual de los contenidos curriculares dentro de los plazos vigentes"[23].

m. "Organiza y dirige el servicio de asesoramiento y monitoreo educativo"[23].

n. "Dirige la orientación al personal docente en la aplicación de las normas técnico pedagógico"[23].

o. “Expide certificados de estudios”[23].

p. “Estimula o aplica las acciones reparadoras, según el caso, a los alumnos del colegio, de conformidad con lo normado en el Reglamento Interno”[23].

q. “Estructura la orientación y bienestar del educando con la participación de docentes y padres de familia”[23].

r. “Potencia el trabajo profesional docente a través de talleres de capacitación”[23].

s. “Coordina con la Institución inmediata superior la cobertura de plazas docentes y administrativas vacantes y el reemplazo oportuno del personal en licencia”[23].

t. “Formula el cuadro de necesidades de bienes y servicios”[23].

u. “Administra la biblioteca, equipos y materiales educativos en coordinación con el personal administrativo”[23].

v. “Preside la comisión encargada de otorgar la administración de kioscos y cafeterías, de acuerdo con las disposiciones vigentes”[23].

w. “Convoca y preside reuniones de trabajo participativo de reflexión pedagógico”[23].

x. “Facilita los medios y recursos educativos para el desarrollo óptimo de las actividades programadas”[23].

y. “Coordina acciones en bien de la I.E. con la Asociación de Padres de Familia”[23].

z. “Promueve la cooperación de instituciones locales y regionales para mejorar los servicios educativos”[23].

aa.“Firma convenios de alianzas estratégicas con instituciones públicas y/o privadas”[23].

bb. “Autoriza de acuerdo a las disposiciones vigentes, el uso eventual de los ambientes y/o equipos de la I.E”[23].

cc.“Preside la Comisión de Gestión de Recursos”[23].

dd. “Informa a la superioridad a los docentes en falta de conformidad a la norma vigente”[23].

ee."Vela por la integridad de todos los miembros de la comunidad educativa dentro de los ambientes de la I.E”[23].

ff. “Genera y promueve espacios y estrategias para el trabajo colaborativo entre los docentes y la reflexión sobre su práctica pedagógica”[23].

gg. Otras inherentes a su cargo.

Responsabilidades del Coordinador de Tutoría:

a. “Realizar el diagnóstico de las necesidades de orientación emocional de los estudiantes”[22].

b. “Elaborar la propuesta de trabajo tutorial para el año lectivo, bajo el enfoque orientador y preventivo adecuándola periódicamente”[22].

c. “Organizar, socializar y sugerir materiales y recursos que permitan dar soporte a las actividades de tutoría”[22].

d. “Desarrollar el acompañamiento a la acción tutorial del Comité de Tutoría de la I.E”[22].

e. “Sistematizar y evaluar la experiencia de la implementación del sistema tutorial cada bimestre para mejorar oportunamente”[22].

f. “Implementar estrategias de articulaciones de la I.E. con las familias de los estudiantes para la mejora de sus capacidades socioemocionales y cognitivas”[22].

g. “Coordinar con el equipo directivo, docentes tutores y auxiliares, la identificación de estudiantes que requiere refuerzo pedagógico y el seguimiento a las actividades de recuperación y reinserción escolar”[22].

Responsabilidades del Coordinador Pedagógico (Letras-Ciencias):

a. “Orientar y promover la participación de los actores de la I.E. en la planificación, ejecución y evaluación curricular del(as) área(s) curricular (res), a partir de las necesidades, características e intereses de los estudiantes y del contexto, considerando las metas de aprendizaje según el CNEB”[22].
b. “Programar acciones para implementar y realizar seguimiento a las estrategias establecidas en el **plan de refuerzo** para alcanzar las metas de aprendizaje proyectadas para cada área curricular, grado y ciclo a su cargo”[22].
c. “Coordinar la elaboración del análisis estadístico de los logros de aprendizaje y el del diagnóstico pedagógico de las áreas curriculares a su cargo”[22].

d. “Analizar de manera colegiada y en forma periódica, los resultados de aprendizaje obtenidos por los estudiantes en las distintas áreas curriculares a su cargo para desarrollar estrategias de mejora de los aprendizajes”[22].
e. “Realizar el monitoreo y acompañamiento pedagógico a los profesores a su cargo y promover estrategias formativas diversas (sesiones compartidas, acompañamiento entre pares, aulas abiertas) para garantizar la mejora de los procesos pedagógicos y los aprendizajes según las normas vigentes”[22].
f. “Promover la integración de las TIC en los procesos pedagógicos y el desarrollo de la labor tutorial con el apoyo de los coordinadores correspondientes”[22].

Responsabilidades del Coordinador de Innovación y Soporte Tecnológico (CIST)

a. “Desarrollar propuestas de formación en alfabetización digital al personal de la institución educativa, en base al diagnóstico para fortalecer estrategias de integración de las herramientas tecnológicas a los procesos de aprendizaje”[22].
b. “Asistir y participar activamente en las reuniones de coordinación con el equipo directivo y convocar a reuniones con profesores de aulas de innovación (si lo hubiere), coordinadores pedagógicos y responsables de aulas”[22].
c. “Coordinar con los docentes de educación para el Trabajo para el uso adecuado de programas informáticos que se empleen en ocupaciones con demanda en el mercado laboral local y regional”[22].
d. “Supervisar las instalaciones y velar por el mantenimiento de los equipos informáticos y de comunicación, asegurando el correcto funcionamiento de los equipos y red de datos”[22].
e. “Realizar el mantenimiento preventivo y correctivo de los equipos informáticos y de comunicación, protegiendo los equipos y detectando necesidades de reparación”[22].
f. “Reportar el estado de los recursos tecnológicos a la dirección de la institución educativa”[22].
g. “Otras actividades inherentes a sus funciones que designe el Órgano de la Dirección de la Institución Educativa”[22].

Responsabilidades del Docente:

a. “Planificar y conducir en forma eficaz el proceso de aprendizaje que favorezcan el desarrollo de competencias en los estudiantes, articulando de manera coherente los aprendizajes programados, sus características individuales, socioculturales, evolutivas y necesidades

especiales, las estrategias y medios seleccionados, para una educación presencial e hibrida"[22].

b. "Evaluar permanentemente el aprendizaje, para tomar decisiones y retroalimentar oportunamente a sus estudiantes teniendo en cuenta las diferencias individuales y los diversos contextos culturales"[22].
c. "Orientar al estudiante y contribuir en su formación integral con respecto a su libertad, autonomía, identidad, creatividad y participación"[22].
d. "Conducir procesos de enseñanza con dominio disciplinar de cada área, el uso de estrategias, recursos educativos y tecnológicos pertinentes para que todos los estudiantes aprendan de manera reflexiva y crítica, estableciendo relaciones interpersonales, asertivas y empáticas, con y entre los estudiantes, basadas en el afecto, la justicia, la confianza, el respeto mutuo y la colaboración"[22].
e. "Constituir con sus pares grupos de inter aprendizaje y participar de programas de formación continua, que favorezcan el trabajo pedagógico, la mejora de la enseñanza y construcción de un clima democrático en la Institución Educativa"[22].
f. "Brindar información y orientación a las familias sobre los procesos y resultados educativos, en un clima de respeto, colaboración y corresponsabilidad en coordinación con el comité de TOE"[22].
g. "Informar a los padres de familia, en el horario y lugar establecido, sobre el desempeño escolar de sus hijos y dialogar con ellos sobre los objetivos educativos y la estrategia"[22].
h. "Participar activamente con actitud democrática, crítica y colaborativa en la gestión de la Institución Educativa, contribuyendo a la construcción y mejora continua del Proyecto Educativo Institucional en el marco del buen desempeño docente con la finalidad de desarrollar aprendizajes de calidad"[22].
i. "Participar en la elaboración, ejecución y evaluación del PEI, PCI, RIN., Plan de Trabajo Anual de la Institución Educativa, MOF"[22].
j. "Programar, desarrollar y evaluar las actividades curriculares, así como las actividades de Tutoría y la formación educativa comunal"[22].
k. "Organizar, ambientar el aula y preparar material educativo con la colaboración de los educandos y padres de familia"[22].
l. "Evaluar el proceso de aprendizaje y la elaboración de la documentación pedagógica"[22].
m. "Mantener actualizada su Carpeta Pedagógica o Portafolio Docente"[22].

Responsabilidades del Auxiliar de Educación:

a. “Apoyar a la labor del profesor en la conducción de actividades específicas y generales de la Institución educativa (formaciones, actos cívicos y otras celebraciones educativas, así como en los recreos) de manera permanente”[22].
b. “Informar oportunamente a la coordinación de tutoría sobre la inasistencia de estudiantes”[22].
c. “Registrar, informar y/o derivar incidencias diarias de los estudiantes, previniendo actos de discriminación y de violencia en la institución”[22].
d. “Desarrollar estrategias de diálogo permanente con los estudiantes, profesores y docentes tutores”[22].
e. “Orientar a los estudiantes sobre actividades pedagógicas correspondientes a cada día, los acuerdos y compromisos relacionados a la convivencia democrática y ordenada en las aulas y otros ambientes de la I.E”[22].
f. “Monitorear el ingreso y salida de los estudiantes de la I.E. con autorización y coordinación de los padres”[22].
g. “Velar el ingreso oportuno de los estudiantes a sus aulas, talleres, laboratorios y otros espacios de aprendizaje en horas programadas”[22].
h. “Atiende a los Padres de Familia sobre asuntos relacionados con la conducta, disciplina y asistencia de sus hijos”[22].
i. “Propicia el mantenimiento de un clima de cooperación, amistad y respeto de los alumnos con los docentes, padres de familia y comunidad”[22].
j. “Fomenta hábitos de disciplina, buenas costumbres, puntualidad, higiene y estudio entre los educandos, así como el correcto y adecuado uso del uniforme escolar”[22].
k. “Controla e informa a su superior inmediato TOE, y a los docentes la inasistencia de los estudiantes otorgando las boletas de justificación”[22].

Responsabilidades del Personal de Vigilancia:

a. “Cautelar la integridad de los miembros de la comunidad educativa dentro de las instalaciones, así como del local escolar”[22].
b. “Verificar y registrar el ingreso y salida de los bienes mobiliarios, materiales y equipos de la Institución Educativa, asimismo, los espacios, ambientes y las personas que se encuentren dentro del local escolar”[22].

c. “Controlar y registrar el movimiento de materiales, herramientas, equipos y bienes de la I.E.”[22].
d. “Efectuar la identificación de las personas en el acceso y en el interior de la Institución Educativa”[22].
e. “Elaborar reporte de las condiciones e incidentes ocurridos en la Institución Educativa”[22].
f. “Detectar y prevenir actos de violencia o de transgresión en la I.E.”[22].
g. “Utilizar credenciales de ingreso para los visitantes de acuerdo al trámite de atención al que se requiera”[22].
h. “Permitir el ingreso de estudiantes más no de acompañantes al local educativo”[22].
i. “Otras actividades inherentes a sus funciones que designe el Órgano Directivo de la Institución Educativa”[22].

Responsabilidades del Psicólogo:

a. “Apoyar la formación de estrategias para la promoción de la Convivencia Democrática e Intercultural en la I.E.”[22].
b. “Acompañar al coordinador de tutoría en el establecimiento y monitoreo de las acciones de tutoría”[22].
c. “Brindar soporte socioemocional a los directivos, coordinadores, profesores en su ejercicio profesional para lograr una atención oportuna y pertinente frente a situaciones y casos que afecten la convivencia institucional y entre los estudiantes en los espacios de recreación y ambientes de aprendizaje”[22].
d. “Brindar soporte socioemocional a los estudiantes y padres de familia a lo largo del año lectivo de manera continua”[22].
e. “Coordinar con los profesores y docentes de tutoría para orientar su accionar en la atención de situaciones de riesgo que puedan afectar a los estudiantes y en los casos de violencia y acoso entre estudiantes”[22].
f. “Promover la elaboración colectiva e implementación de normas de convivencia para mejorar el ambiente educativo y los valores democráticos en la Institución Educativa”[22].
g. “Coordinar con el equipo directivo la organización de actividades educativas con padres y madres de familia y relacionados a los intereses y necesidades de los estudiantes para su formación integral”[22].
h. “Realizar visitas domiciliarias a los estudiantes que presentan problemas académicos y conductuales dentro de la I.E.”[22].

CORE BUSINESS:

La prestación del servicio comienza cuando el estudiante requiere el logro de aprendizajes de acuerdo a sus necesidades y realiza su matrícula en la modalidad que le corresponde; para ello la institución educativa se encarga de organizar el servicio educativo mediante matrículas, calendarización del año escolar, desarrollo de la programación curricular, implementar el trabajo colegiado y realizar el monitoreo pedagógico; existen dos modalidades de matrícula, una es de forma automática cuando el estudiante ya es parte de la institución y solo requiere ser promovido de grado y la otra modalidad corresponde a una matrícula de forma presencial por medio del llenado de un formulario entregado por la secretaria de la institución, esta a su vez matricula al alumno de acuerdo al grado académico y nivel de estudios en la plataforma SIAGIE, también se pueden realizar traslados que son similares a las matrículas de forma presencial, entregando un formulario a rellenar. De acuerdo a las nuevas circunstancias que vienen aconteciendo en nuestro entorno, la modalidad de matrícula presencial ha sido reemplazada por medio de llamadas telefónicas al igual que los traslados, de esta forma se consolidan tres modalidades de matrícula, así como también dos modalidades de traslados; prosigue la calendarización del año escolar en donde la plan jerárquica conjuntamente con los docentes coordinan como se llevará a cabo todo el periodo académico; el desarrollo de la programación curricular es también coordinado entre docentes y plana jerárquica con la finalidad de actualizar el PEI, RIN, PAT y las unidades de aprendizaje respondiendo de este modo a los intereses, saberes y necesidades del estudiante, posteriormente se implementa el trabajo colegiado y el monitoreo pedagógico a fin de brindar una educación de calidad. El proceso de gestión de los aprendizajes es llevado a cabo por dos actores principales; el docente y estudiante, donde el docente realiza de manera diaria una sesión de aprendizaje el cual será guiada por la unidad de aprendizaje realizada anteriormente y verificada por el coordinador y validada por el subdirector académico a fin de corroborar la secuencia de actividades establecidas con el fin de brindar una educación de calidad a sus estudiantes, también se realiza el reforzamiento de los aprendizajes con el objetivo de mejorar la experiencia del estudiante y que no queden dudas del aprendizaje logrado. Finalmente, se evalúan los logros de aprendizaje de forma trimestral para luego registrarlos en un registro auxiliar el cual será validado por el subdirector para posteriormente subir los calificativos al SIAGIE, de esta manera se logra que el estudiante pueda ser promovido de nivel.

PARTES INTERESADAS:

a. CLIENTES: Estudiantes.

b. COLABORADORES: Brigada y/o Policía Escolar, docentes, padres de Familia, director, coordinadores pedagógicos, psicólogo, CIST, auxiliar y vigilantes.

c. REGULADORES: Ugel Huancayo, DREJ (Dirección Regional de Educación Junín), Ministerio de Educación.

d. PROVEEDORES: Ministerio de Educación, padres de familia.

CLASIFICACIÓN DE PROCESOS:

- **Procesos misionales u operativos:** Procesos que permiten generar el producto/ servicio que se entrega al cliente a fin de satisfacer sus necesidades.
- **Procesos de apoyo:** Procesos que abarcan las actividades necesarias para el correcto funcionamiento de los procesos operativos.
- **Procesos Estratégicos:** Procesos destinados a definir y controlar las metas de la organización, sus estrategias y políticas.

DEFINICIÓN DE LOS PROCESOS:

PROCESOS ESTRATÉGICOS

- **Desarrollar planeamiento institucional:** Comprende todas las actividades de análisis y formulación del PEI, RIN y PAT.
- **Evaluar la gestión escolar:** Es el proceso estratégico orientado a desarrollar lineamientos, herramientas y métodos que permitan promover la gestión escolar.
- **Gestionar el desarrollo e Innovación Institucional:** Comprende la articulación de proyectos, promover alianzas institucionales.

PROCESOS MISIONALES

- **ORGANIZAR EL SERVICIO EDUCATIVO:**

  Matricular Estudiantes: Proceso de matrícula automática o presencial.

  Realizar la calendarización del año escolar: Calendario académico

  Desarrollar la programación curricular: Proceso de actualizar PEI, PAT, RIN, Unidades de aprendizajes.

Realizar el monitoreo pedagógico: Supervisar los componentes pedagógicos

Implementar el trabajo colegiado: Proceso de lluvia de ideas a fin de conocer deficiencias en torno a los aprendizajes de los estudiantes.

- **GENERAR CONDICIONES PARA LA CONVIVENCIA ESCOLAR**

  Prevenir y resolver conflictos: Comprende las actividades a identificar y prever conflictos a fin de desarrollar un buen desempeño escolar.

  Vincular la escuela con la sociedad: Comprende actividades de orientación tanto a padres de familia como a estudiantes.

- **GESTIONAR LOS APRENDIZAJES**

  Desarrollar Sesiones de aprendizaje: Las sesiones de aprendizaje se realizan todos los días por el docente, el cual guía por la unidad de aprendizaje.

  Realizar acompañamiento integral del estudiante: Comprende actividades de acompañamiento, guiando a los estudiantes en su aprendizaje.

  Evaluar aprendizajes: Este proceso consiste en tomar exámenes trimestrales a los estudiantes.

PROCESOS DE APOYO

- **Almacenar y conservar los bienes y recursos educativos:** Comprende las actividades administración de bienes y el control del patrimonio.
- **Administrar los recursos humanos:** Comprende las actividades de administración del personal de la institución, vinculación y desvinculación del personal.
- **Administrar recursos económicos:** Comprende las actividades de recaudación de los ingresos, ejecución de egresos de fondos y rendición de cuentas.
- **Conservar Infraestructura y servicios educativos:** Comprende los procesos de soporte contundente a disponer de los bienes y servicios necesarios para el adecuado funcionamiento de la institución.

MAPA DE PROCESOS

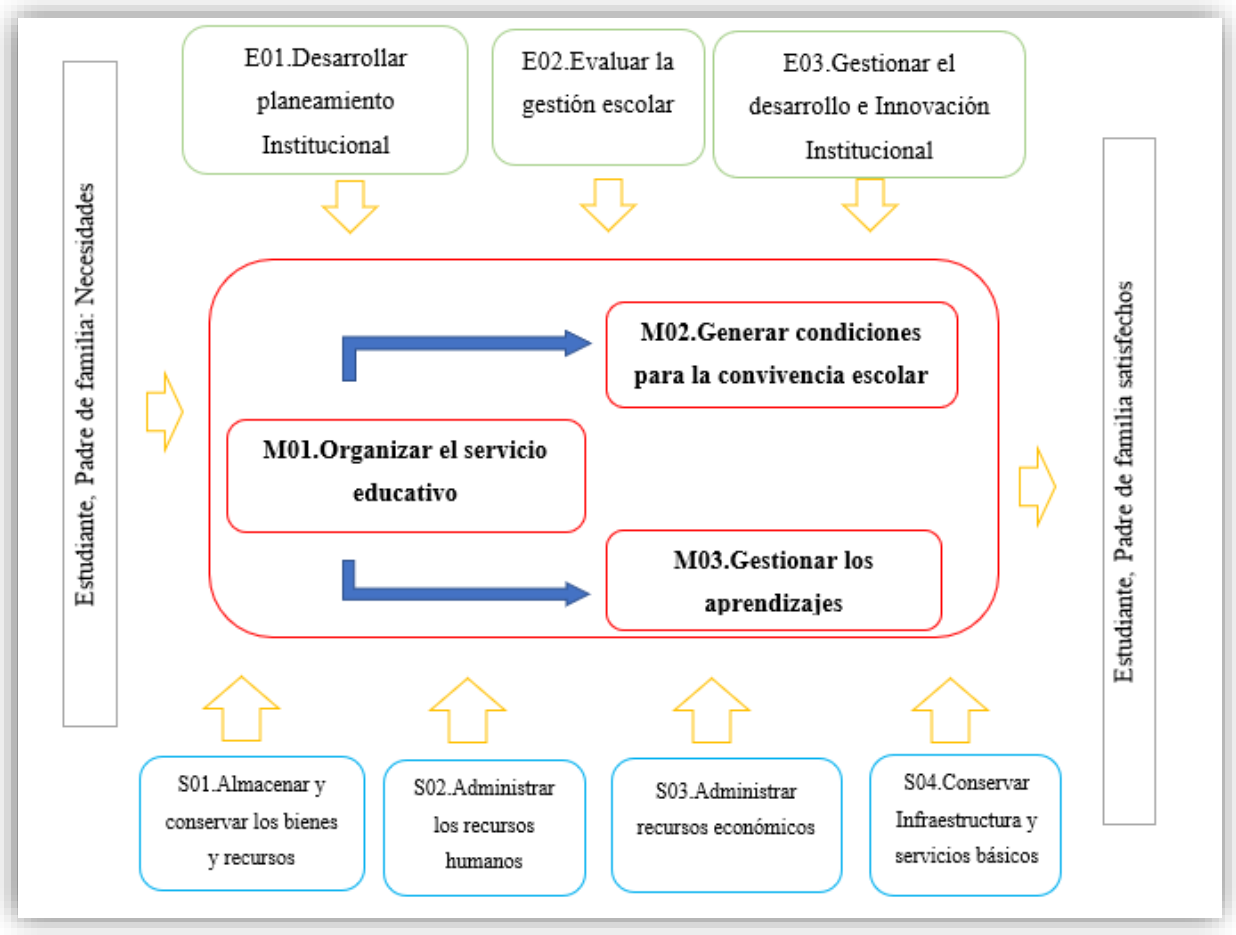

Fig. 11. Mapa de Procesos I.E. Francisco de Zela.

INVENTARIO DE ACTIVOS CRÍTICOS

TABLA V INVENTARIO DE ACTIVOS CRÍTICOS

N°	CÓDIGO	NOMBRE DEL ACTIVO	TIPO	MARCA	MODELO	SERIE	UBICACIÓN	RESPONSABLE
1	FZ0001	LIBRO DE ACTAS	ACTIVO ESENCIAL				DIRECCIÓN	DIRECTOR
2	FZ0002	AMPLIFICADOR DE AUDIO	HARDWARE	POTENZA			DIRECCIÓN	DIRECTOR
3	FZ0003	ARCHIVADOR DE MADERA	EQUIPAMIENTO AUXILIAR				DIRECCIÓN	DIRECTOR
4	FZ0004	ARCHIVADOR DE METAL	EQUIPAMIENTO AUXILIAR				ALMACÉN	PERSONAL DE VIGILANCIA
5	FZ0005	ARMARIO DE METAL	EQUIPAMIENTO AUXILIAR				DIRECCIÓN	DIRECTOR
6	FZ0006	ARMARIO DE METAL	EQUIPAMIENTO AUXILIAR				AULA 01	DOCENTE ASIGNADO
7	FZ0007	ARMARIO DE METAL	EQUIPAMIENTO AUXILIAR				AULA INNOVACIÓN	CIST
8	FZ0008	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC11405E74	AULA 01	DOCENTE ASIGNADO
9	FZ0009	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC11405EC9	AULA 01	DOCENTE ASIGNADO
10	FZ00010	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC11405ED2	AULA 01	DOCENTE ASIGNADO
11	FZ00011	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC11405ED6	AULA 01	DOCENTE ASIGNADO

12	FZ00012	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC11405EE4	AULA 01	DOCENTE ASIGNADO
13	FZ00013	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC11402A66	AULA 01	DOCENTE ASIGNADO
14	FZ00014	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC11403322	AULA 01	DOCENTE ASIGNADO
15	FZ00015	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC114034A5	AULA 01	DOCENTE ASIGNADO
16	FZ00016	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC114034AD	AULA 01	DOCENTE ASIGNADO
17	FZ00017	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC11403553	AULA 01	DOCENTE ASIGNADO
18	FZ00018	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC11405E90	AULA 01	DOCENTE ASIGNADO
19	FZ00019	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC11405EFE	AULA 01	DOCENTE ASIGNADO
20	FZ00020	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC11405EFF	AULA 01	DOCENTE ASIGNADO
21	FZ00021	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC11405F71	AULA 01	DOCENTE ASIGNADO
22	FZ00022	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC11405F74	AULA 01	DOCENTE ASIGNADO
23	FZ00023	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC11405DDD	AULA 01	DOCENTE ASIGNADO

24	FZ00024	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC11405DDF	AULA 01	DOCENTE ASIGNADO
25	FZ00025	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC11405DE3	AULA 01	DOCENTE ASIGNADO
26	FZ00026	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC11405DF1	AULA 01	DOCENTE ASIGNADO
27	FZ00027	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC11405DFB	AULA 01	DOCENTE ASIGNADO
28	FZ00028	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC1290183E	AULA 01	DOCENTE ASIGNADO
29	FZ00029	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC12901912	AULA 01	DOCENTE ASIGNADO
30	FZ00030	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC12901AB0	AULA 01	DOCENTE ASIGNADO
31	FZ00031	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC12901ADD	AULA 01	DOCENTE ASIGNADO
32	FZ00032	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC12901AE2	AULA 01	DOCENTE ASIGNADO
33	FZ00033	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	OLPC	XO-1	SHC12901ADF	AULA 01	DOCENTE ASIGNADO
34	FZ00034	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	HP 450	8CG7133CQR	DIRECCIÓN	DIRECTOR
35	FZ00035	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	HP 450	8CG7133CLH	DIRECCIÓN	DIRECTOR

36	FZ00036	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND538FFB4	AULA INNOVACIÓN	CIST
37	FZ00037	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND53967YF	AULA INNOVACIÓN	CIST
38	FZ00038	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND53964NL	AULA INNOVACIÓN	CIST
39	FZ00039	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND53927B2	AULA INNOVACIÓN	CIST
40	FZ00040	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND53921QK	AULA INNOVACIÓN	CIST
41	FZ00041	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND53968SX	AULA INNOVACIÓN	CIST
42	FZ00042	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND5390H10	AULA INNOVACIÓN	CIST
43	FZ00043	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND53962ZX	AULA INNOVACIÓN	CIST
44	FZ00044	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND5390H7N	AULA INNOVACIÓN	CIST
45	FZ00045	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND5390KGH	AULA INNOVACIÓN	CIST
46	FZ00046	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND53903GW	AULA INNOVACIÓN	CIST
47	FZ00047	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND5390M4D	AULA INNOVACIÓN	CIST

48	FZ00048	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND5391Z7C	AULA INNOVACIÓN	CIST
49	FZ00049	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND5390R3H	AULA INNOVACIÓN	CIST
50	FZ00050	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND5390L8N	AULA INNOVACIÓN	CIST
51	FZ00051	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND5390CLL	AULA INNOVACIÓN	CIST
52	FZ00052	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND5390GLM	AULA INNOVACIÓN	CIST
53	FZ00053	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND538DXM9	AULA INNOVACIÓN	CIST
54	FZ00054	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND5390SK4	AULA INNOVACIÓN	CIST
55	FZ00055	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND53962TJ	AULA INNOVACIÓN	CIST
56	FZ00056	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND53966NL	AULA INNOVACIÓN	CIST
57	FZ00057	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND538FF54	AULA INNOVACIÓN	CIST
58	FZ00058	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND5390TTE	AULA INNOVACIÓN	CIST
59	FZ00059	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND5391CB8	AULA INNOVACIÓN	CIST

60	FZ00060	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND5390MHN	AULA INNOVACIÓN	CIST
61	FZ00061	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND538F661	AULA INNOVACIÓN	CIST
62	FZ00062	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND53908WM	AULA INNOVACIÓN	CIST
63	FZ00063	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND53904LS	AULA INNOVACIÓN	CIST
64	FZ00064	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND53917DT	AULA INNOVACIÓN	CIST
65	FZ00065	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND5390K0K	AULA INNOVACIÓN	CIST
66	FZ00066	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND54026H1	AULA INNOVACIÓN	CIST
67	FZ00067	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND5393J2W	AULA INNOVACIÓN	CIST
68	FZ00068	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND53962W7	AULA INNOVACIÓN	CIST
69	FZ00069	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND5392QSJ	AULA INNOVACIÓN	CIST
70	FZ00070	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND5392B6V	AULA INNOVACIÓN	CIST
71	FZ00071	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND538FD4L	AULA INNOVACIÓN	CIST

72	FZ00072	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND53967NT	AULA INNOVACIÓN	CIST
73	FZ00073	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND5390DVK	AULA INNOVACIÓN	CIST
74	FZ00074	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND53929KN	AULA INNOVACIÓN	CIST
75	FZ00075	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND53967T8	AULA INNOVACIÓN	CIST
76	FZ00076	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND61421RC	DIRECCIÓN	DIRECTOR
77	FZ00077	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND61421WT	DIRECCIÓN	DIRECTOR
78	FZ00078	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6084ZYS	AULA 01	DOCENTE ASIGNADO
79	FZ00079	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6080B2S	AULA INNOVACIÓN	CIST
80	FZ00080	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6081JZ9	AULA 01	DOCENTE ASIGNADO
81	FZ00081	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6080HPP	AULA INNOVACIÓN	CIST
82	FZ00082	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6080BLY	AULA INNOVACIÓN	CIST
83	FZ00083	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6080LFW	AULA 01	DOCENTE ASIGNADO

84	FZ00084	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND60807JM	AULA INNOVACIÓN	CIST
85	FZ00085	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6080GG6	AULA 01	DOCENTE ASIGNADO
86	FZ00086	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6080GWL	AULA 01	DOCENTE ASIGNADO
87	FZ00087	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND608182L	AULA 01	DOCENTE ASIGNADO
88	FZ00088	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND608079Y	AULA 01	DOCENTE ASIGNADO
89	FZ00089	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND60806DM	AULA 01	DOCENTE ASIGNADO
90	FZ00090	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND60803SB	AULA 01	DOCENTE ASIGNADO
91	FZ00091	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND60803JF	AULA 01	DOCENTE ASIGNADO
92	FZ00092	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6084ZPK	AULA 01	DOCENTE ASIGNADO
93	FZ00093	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND60802X1	AULA INNOVACIÓN	CIST
94	FZ00094	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6080KN2	AULA 01	DOCENTE ASIGNADO
95	FZ00095	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND60851YT	AULA INNOVACIÓN	CIST

96	FZ00096	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6080GNV	AULA 01	DOCENTE ASIGNADO
97	FZ00097	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6081RJL	AULA INNOVACIÓN	CIST
98	FZ00098	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6080K2V	AULA INNOVACIÓN	CIST
99	FZ00099	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND60814VH	AULA INNOVACIÓN	CIST
100	FZ000100	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6080354	AULA INNOVACIÓN	CIST
101	FZ000101	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6080LXF	AULA INNOVACIÓN	CIST
102	FZ000102	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND60804YZ	AULA 01	DOCENTE ASIGNADO
103	FZ000103	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6080KKY	AULA INNOVACIÓN	CIST
104	FZ000104	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND60806YR	AULA INNOVACIÓN	CIST
105	FZ000105	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6080727	AULA INNOVACION	CIST
106	FZ000106	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6081BQ8	AULA INNOVACIÓN	CIST
107	FZ000107	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6081CRQ	AULA INNOVACIÓN	CIST

108	FZ000108	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6081CN3	AULA INNOVACIÓN	CIST
109	FZ000109	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6081C4B	AULA 01	DOCENTE ASIGNADO
110	FZ000110	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND60805YV	AULA 01	DOCENTE ASIGNADO
111	FZ000111	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND60805W8	AULA 01	DOCENTE ASIGNADO
112	FZ000112	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND60809V1	AULA 01	DOCENTE ASIGNADO
113	FZ000113	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6081RXZ	AULA 01	DOCENTE ASIGNADO
114	FZ000114	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND608598X	AULA 01	DOCENTE ASIGNADO
115	FZ000115	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6080413	AULA 01	DOCENTE ASIGNADO
116	FZ000116	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND60806XM	AULA 01	DOCENTE ASIGNADO
117	FZ000117	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND60801ZQ	AULA 01	DOCENTE ASIGNADO
118	FZ000118	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6080Y19	AULA 01	DOCENTE ASIGNADO
119	FZ000119	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6080JCV	AULA 01	DOCENTE ASIGNADO

120	FZ000120	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6080FMN	AULA 01	DOCENTE ASIGNADO
121	FZ000121	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND60820GZ	AULA 01	DOCENTE ASIGNADO
122	FZ000122	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND60806Z4	AULA 01	DOCENTE ASIGNADO
123	FZ000123	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND608078W	AULA 01	DOCENTE ASIGNADO
124	FZ000124	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND6080V47	AULA 01	DOCENTE ASIGNADO
125	FZ000125	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	250 G4	CND60853J4	AULA 01	DOCENTE ASIGNADO
126	FZ000126	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	450	5CG3191Z7K	ALMACÉN	PERSONAL DE VIGILANCIA
127	FZ000127	COMPUTADORA PERSONAL PORTÁTIL	HARDWARE	HP	450	5CG3234QR3	ALMACÉN	PERSONAL DE VIGILANCIA
128	FZ000128	CONSOLA PARA CONTROL DE AUDIO	HARDWARE				ALMACÉN	PERSONAL DE VIGILANCIA
129	FZ000129	DISCO DURO EXTERNO	SOPORTE DE INFORMACIÓN	DELL	92NKHNA	NZO5A5BH	AULA INNOVACIÓN	CIST
130	FZ000130	EQUIPO DE SONIDO	HARDWARE	ALTRON	G-6000	ALMIN106906	DIRECCIÓN	DIRECTOR
131	FZ000131	EQUIPO DE SONIDO	HARDWARE	S86	HB1028		AULA INNOVACIÓN	CIST
132	FZ000132	ESTABILIZADOR	EQUIPAMIENTO AUXILIAR	CDP	AVR10061 1200W		DIRECCIÓN	DIRECTOR

133	FZ000133	ESTABILIZADOR	EQUIPAMIENTO AUXILIAR	CDP	AVR1006I		AULA 01	DOCENTE ASIGNADO
134	FZ000134	ESTABILIZADOR	EQUIPAMIENTO AUXILIAR	FORTEX	FOR-1200		AULA 01	DOCENTE ASIGNADO
135	FZ000135	ESTABILIZADOR	EQUIPAMIENTO AUXILIAR	FORTEX	FOR-1200		AULA 01	DOCENTE ASIGNADO
136	FZ000136	FOTOCOPIADORA EN GENERAL	HARDWARE	KONICA MINOLTA	BIZHUB 185		DIRECCIÓN	DIRECTOR
137	FZ000137	IMPRESORA A INYECCIÓN DE TINTA	HARDWARE	BROTHER			DIRECCIÓN	DIRECTOR
138	FZ000138	IMPRESORA LASER	HARDWARE	HP 1020	Q5911A	BRCS7BPG0Y	DIRECCIÓN	DIRECTOR
139	FZ000139	REPRODUCTOR DE VIDEO	HARDWARE	ALTRON	DVD2030	ALDVD121004355	DIRECCIÓN	DIRECTOR
140	FZ000140	REPRODUCTOR DE VIDEO	HARDWARE	ALTRON	DVD2030	ALDVD121004356	DIRECCIÓN	DIRECTOR
141	FZ000141	SERVIDOR	HARDWARE	LENOVO		SMJ046POM	AULA INNOVACIÓN	CIST
142	FZ000142	PROYECTOR MULTIMEDIA	HARDWARE	BENQ	MS500	PD32C04019000-S	AULA 04	DOCENTE ASIGNADO
143	FZ000143	PROYECTOR MULTIMEDIA	HARDWARE	VIEWSONIC	PJD5153 3300LUM	U4P160101329	AULA 05	DOCENTE ASIGNADO
144	FZ000144	PROYECTOR MULTIMEDIA	HARDWARE	SONY	VPL-EX235	S0151121725	AULA 03	DOCENTE ASIGNADO
145	FZ000145	PROYECTOR MULTIMEDIA	HARDWARE	SONY	VPL-EX235	S015112169B	AULA 06	DOCENTE ASIGNADO
146	FZ000146	PROYECTOR MULTIMEDIA	HARDWARE	EPSON	POWERLITE S39	X52M852053L	AULA 10	DOCENTE ASIGNADO

147	FZ000147	PROYECTOR MULTIMEDIA	HARDWARE	EPSON	POWERLITE S39	X52M852051L	AULA 11	DOCENTE ASIGNADO
148	FZ000148	PROYECTOR MULTIMEDIA	HARDWARE	EPSON	POWERLITE S39	X52M852041X	AULA 09	DOCENTE ASIGNADO
149	FZ000149	PROYECTOR MULTIMEDIA	HARDWARE	EPSON	POWERLITE S39	X52M852054F	AULA 08	DOCENTE ASIGNADO
150	FZ000150	PROYECTOR MULTIMEDIA	HARDWARE	EPSON	POWERLITE S39	X52M852061T	AULA 02	DOCENTE ASIGNADO
151	FZ000151	PROYECTOR MULTIMEDIA	HARDWARE	EPSON	POWERLITE S39	X52M852058Q	AULA 07	DOCENTE ASIGNADO
152	FZ000152	PROYECTOR MULTIMEDIA	HARDWARE	EPSON	POWERLITE S39	X52M852055J	AULA INNOVACIÓN	CIST
153	FZ000153	TELEVISOR A COLORES	HARDWARE	SAMSUNG 29"	CL29K5MQ	B16P3CCLG02019F	DIRECCIÓN	DIRECTOR
154	FZ000154	TELEVISOR LED	HARDWARE	SAMSUNG	UN48J5500AG	03Q93CXH200176	AULA 03	DOCENTE ASIGNADO
155	FZ000155	TELEVISOR LED	HARDWARE	SAMSUNG	UN48J5500AG	03Q93CXH301889	AULA 07	DOCENTE ASIGNADO
156	FZ000156	TELEVISOR LED	HARDWARE	SAMSUNG	UN48J5500AG	03Q93CXH301787	AULA 11	DOCENTE ASIGNADO
157	FZ000157	TELEVISOR LED	HARDWARE	SAMSUNG	UN48J5500A6	03Q93CXH301787	AULA 09	DOCENTE ASIGNADO
158	FZ000158	TELEVISOR LED	HARDWARE	SAMSUNG 48"	UN48J5500A6	03Q93CVJ201049	AULA 08	DOCENTE ASIGNADO

159	FZ000159	UNIDAD CENTRAL DE PROCESO - CPU	HARDWARE	MICRONICS	AMD ATHLON II	6B1638	DIRECCIÓN	DIRECTOR
160	FZ000160	UNIDAD CENTRAL DE PROCESO - CPU	HARDWARE	MICRONICS	AMD ATHLON II	9V04486610537	AULA 01	DOCENTE ASIGNADO
161	FZ000161	UNIDAD CENTRAL DE PROCESO - CPU	HARDWARE	MICRONICS	AMD ATHLON II	9R99456G10331	AULA 01	DOCENTE ASIGNADO
162	FZ000162	UNIDAD CENTRAL DE PROCESO - CPU	HARDWARE	MICRONICS	AMD ATHLON II	9V04486G10009	SECRETARÍA	SECRETARIA
163	FZ000163	CÁMARA DE VIGILANCIA	HARDWARE	HIKVISION	DS-J142	7104HQHIK1F	PATIO	DIRECTOR
164	FZ000164	CÁMARA DE VIGILANCIA	HARDWARE	HIKVISION	DS-J143	7104HQHIK2J	PUERTA ENTRADA	DIRECTOR
165	FZ000165	CÁMARA DE VIGILANCIA	HARDWARE	HIKVISION	DS-J144	7104HQHIK3J	PUERTA DIRECCIÓN	DIRECTOR
166	FZ000166	CÁMARA DE VIGILANCIA	HARDWARE	HIKVISION	DS-J145	7104HQHIK4G	PATIO	DIRECTOR
167	FZ000167	CÁMARA DE VIGILANCIA	HARDWARE	HIKVISION	DS-J146	7104HQHIK3F	PATIO	DIRECTOR
168	FZ000168	CÁMARA DE VIGILANCIA	HARDWARE	HIKVISION	DS-J147	7104HQHIK5F	PATIO	DIRECTOR
169	FZ000169	LIBRO DE INCIDENCIAS	DATOS /INFORMACIÓN				DIRECCIÓN	DIRECTOR
170	FZ000170	CUADERNO DE ATENCIONES	DATOS /INFORMACIÓN	ARTESCO	A4		COORD. TUTORÍA	COORDINADOR DE TUTORÍA
171	FZ000171	CUADERNO DE INCIDENCIAS	DATOS /INFORMACIÓN	ARTESCO	A4		PSICOLOGÍA	PSICÓLOGO
172	FZ000172	ACTA DE EVALUACIÓN Y CERTIFICADO DE ESTUDIOS	DATOS /INFORMACIÓN				DIRECCIÓN	DIRECTOR

173	FZ000173	ACTA DE EVALUACIÓN Y CERTIFICADO DE ESTUDIOS	DATOS /INFORMACIÓN				DIRECCIÓN	DIRECTOR
174	FZ000174	ACTA DE EVALUACIÓN Y CERTIFICADO DE ESTUDIOS	DATOS /INFORMACIÓN				DIRECCIÓN	DIRECTOR
175	FZ000175	ACTA DE EVALUACIÓN Y CERTIFICADO DE ESTUDIOS	DATOS /INFORMACIÓN				DIRECCIÓN	DIRECTOR
176	FZ000176	ACTA DE EVALUACIÓN Y CERTIFICADO DE ESTUDIOS	DATOS /INFORMACIÓN				DIRECCIÓN	DIRECTOR
177	FZ000177	FICHAS DE MONITOREO CIENCIAS	DATOS /INFORMACIÓN				COORD. CIENCIAS	COORDINADOR DE CIENCIAS
178	FZ000178	FICHAS DE MONITOREO LETRAS	DATOS /INFORMACIÓN				COORD. LETRAS	COORDINADOR DE LETRAS
179	FZ000179	REG. DE ASISTENCIA TRABAJADORES	DATOS /INFORMACIÓN				DIRECCIÓN	DIRECTOR
180	FZ000180	REG. DE ASISTENCIA ESTUDIANTES	DATOS /INFORMACIÓN				CASETA AUXILIAR	AUXILIAR
181	FZ000181	MEMORÁNDUMS	DATOS /INFORMACIÓN				DIRECCIÓN	DIRECTOR
182	FZ000182	BOLETA DE NOTAS	DATOS /INFORMACIÓN				DIRECCIÓN	DIRECTOR
183	FZ000183	CONTRASEÑAS DE EQUIPOS	DATOS /INFORMACIÓN				DIRECCIÓN	CIST
184	FZ000184	CONTRASEÑAS DE PLATAFORMAS	DATOS /INFORMACIÓN				DIRECCIÓN	DIRECTOR

185	FZ000185	REGLAMENTO INTERNO INSTITUCIONAL	DATOS /INFORMACIÓN				DIRECCIÓN	DIRECTOR
186	FZ000186	PLAN ANUAL DE TRABAJO	DATOS /INFORMACIÓN				DIRECCIÓN	DIRECTOR
187	FZ000187	PROYECTO EDUCATIVO INSTITUCIONAL	DATOS /INFORMACIÓN				DIRECCIÓN	DIRECTOR
188	FZ000188	SISTEMA OPERATIVO WIN10	SOFTWARE				AULA 01	CIST
189	FZ000189	SISTEMA OPERATIVO WIN8 PRO	SOFTWARE				AULA INNOVACIÓN	CIST
190	FZ000190	MICROSOFT OFFICE 2013	SOFTWARE				AULA INNOVACIÓN	CIST
191	FZ000191	MICROSOFT OFFICE 2016	SOFTWARE				AULA 01	CIST
192	FZ000192	SCRATCH V3	SOFTWARE				AULA INNOVACIÓN	CIST
193	FZ000193	XMIND	SOFTWARE				AULA INNOVACION	CIST
194	FZ000194	CMAPTOOLS	SOFTWARE				AULA INNOVACIÓN	CIST
195	FZ000196	MODEM ROUTER	HARDWARE	TPLINK	DAP2360	8843903133	DIRECCIÓN	DIRECTOR

A.2. NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

TABLA VI NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

INSTITUCIÓN EDUCATIVA FRANCISCO DE ZELA	**PARTES INTERESADAS NECESIDADES Y EXPECTATIVAS**	CÓDIGO: FZ-002-2024 EMISIÓN: 23-01-24 VERSIÓN_ 01 Página 1
PARTE INTERESADA	**NECESIDAD(ES)**	**EXPECTATIVA(S)**
DIRECCIÓN	Desarrollar e implementar políticas claras de seguridad de la información que aborden la protección de datos sensibles y definan roles y responsabilidades.	La dirección espera contar con políticas bien definidas que establezcan estándares de seguridad, normas de conducta y procedimientos para garantizar la integridad, confidencialidad y disponibilidad de la información.
	Crear un plan de continuidad del negocio que contemple cómo mantener las operaciones en caso de interrupciones, ya sea por desastres naturales, ciberataques u otras contingencias.	La dirección busca contar con un plan detallado que minimice el tiempo de inactividad en situaciones de crisis, asegurando la continuidad de las actividades educativas y administrativas.
	Realizar evaluaciones regulares de riesgos de seguridad y auditorías para identificar posibles vulnerabilidades y áreas de mejora.	La dirección espera informes detallados que destaquen las amenazas potenciales, identifiquen áreas de riesgo y proporcionen recomendaciones para fortalecer la seguridad de la información.

	Implementar programas de concientización y capacitación en seguridad de la información para todo el personal, incluidos docentes, administrativos y estudiantes.	La dirección espera que el personal esté bien informado sobre las mejores prácticas de seguridad, reconozca posibles amenazas y contribuya activamente a la protección de la información.
	Realizar inversiones en tecnologías de seguridad, como firewalls, sistemas de detección de intrusiones y antivirus, para proteger la infraestructura tecnológica del colegio.	La dirección busca garantizar que la infraestructura tecnológica esté respaldada por herramientas de seguridad efectivas y actualizadas que mitiguen los riesgos asociados con amenazas cibernéticas.
DOCENTES	Capacitaciones en seguridad de la información	Capacitación permanente
	Ingresar de manera segura a las plataformas digitales del estado (SIAGIE, SIMON, PERUEDUCA)	Ingresar a las plataformas del estado sin riesgo a exponer sus datos confidenciales
	Almacenamiento de información	Almacenar información en sus computadoras portátiles de manera segura y sin riesgo a pérdida
	Gestionar sus contraseñas de manera segura	Gestionar contraseñas de manera que no tengan que recordar demasiadas y sin exponerse a ser víctimas de usurpación.

	Protección de datos personales	Manejar información personal y académica de sus estudiantes
	Seguridad en dispositivos	Utilizar dispositivos electrónicos para preparar y dar clases, así como comunicarse con sus estudiantes y colegas.
ADMINISTRATIVOS	Gestión segura de la información financiera	Manejar información financiera como, nóminas, presupuestos, pagos de apafas, de manera segura
	Control de acceso a sistemas administrativos solo a personal autorizado	Garantizar que solo el personal autorizado tenga la capacidad de acceder y modificar datos de ingreso a los sistemas administrativos
	Seguridad de comunicaciones internas	Mantener la confidencialidad de la comunicación, esto implica el uso de correos electrónicos seguros, encriptación de mensajes y concienciación sobre posibles amenazas de ingeniería social.
	Respaldo y recuperación de datos administrativos	La información administrativa, como registros de estudiantes y personal, así como documentación legal, debe contar con sistemas efectivos de respaldo y recuperación
	Actualizaciones de Seguridad y Mantenimiento de Software	Software utilizado por los administrativos actualizado para beneficiarse de las últimas correcciones de seguridad.
PERSONAL DE VIGILANCIA	Supervisar y controlar el acceso a áreas sensibles, como salas de servidores, oficinas	Se espera que el personal de vigilancia mantenga una vigilancia constante en las áreas sensibles, asegurándose de que solo las personas autorizadas

	administrativas y archivos.	tengan acceso y reportando cualquier actividad sospechosa.
	Conocer las principales amenazas que puedan comprometer la seguridad de la información	Entrenamiento para reconocer situaciones anómalas, responder a emergencias y comunicar de manera efectiva con el personal de seguridad y la dirección del colegio.
	Monitoreo de cámaras de seguridad de la institución	Realizar un monitoreo constante de las cámaras de seguridad, revisando grabaciones cuando sea necesario, y reportando cualquier actividad inusual o sospechosa.
	Inversión en equipos de seguridad de acceso a las diferentes áreas de la institución	Todas las áreas de la Institución Educativa deben cumplir con los requisitos mínimos de seguridad como: Cerraduras de seguridad, cámaras de vigilancia, protección contra incendios.
ESTUDIANTES	Protección de la privacidad de la información personal, como nombres, direcciones y datos de contacto.	Los estudiantes esperan que la institución implemente medidas efectivas para salvaguardar sus datos personales, asegurando que solo el personal autorizado tenga acceso y que la información no se comparta sin su consentimiento.
	Entender los conceptos básicos de seguridad digital y prácticas seguras en línea.	Los estudiantes esperan recibir educación sobre cómo proteger sus datos personales, reconocer posibles amenazas en línea y utilizar de manera segura las plataformas digitales proporcionadas por la institución educativa.
	Acceso seguro a plataformas en línea	Los estudiantes esperan que se implementen medidas de seguridad,

	utilizadas para el aprendizaje y la colaboración.	como autenticación segura, para garantizar que solo los usuarios autorizados tengan acceso a los recursos educativos en línea y que sus datos estén protegidos.
	Protección contra el ciberacoso y la intimidación en línea.	Los estudiantes esperan que la institución tenga políticas claras contra el ciberacoso, implemente medidas de prevención y proporcione recursos y apoyo para aquellos que experimenten situaciones de acoso en línea.
	Privacidad en entornos virtuales de aprendizaje y colaboración.	Los estudiantes esperan que se establezcan normas claras para el uso de herramientas colaborativas en línea, asegurando que su participación en discusiones y la presentación de trabajos no comprometan su privacidad y seguridad.
PADRES DE FAMILIA	Acceso seguro a la información académica de sus hijos, como calificaciones, asistencia y comunicaciones escolares.	Los padres esperan que la institución proporcione plataformas seguras para acceder a la información académica de sus hijos, con medidas de autenticación robustas y la garantía de que la información está protegida.
	Comunicarse de manera segura con la institución sobre asuntos académicos y administrativos.	Los padres esperan que se implementen canales de comunicación seguros, como plataformas de mensajería segura y cuentas oficiales de la institución, para garantizar que la información compartida sobre sus hijos y temas institucionales sean confidenciales y seguros.

	Entender los conceptos de seguridad digital y cómo proteger la información de sus hijos en línea.	Los padres esperan que la institución educativa proporcione recursos y capacitación sobre seguridad digital para que puedan entender y abordar de manera efectiva los riesgos en línea que puedan afectar a sus hijos.
	Garantizar la protección de los datos personales de la familia en registros escolares y comunicaciones.	Los padres esperan que la institución tenga políticas claras de privacidad, restricciones de acceso a datos personales y medidas de seguridad para proteger la información de la familia.
	Participar de manera segura en eventos y reuniones virtuales organizados por la institución.	Los padres esperan que se tomen medidas para garantizar la seguridad en las plataformas utilizadas para eventos virtuales, como reuniones de padres y conferencias en línea, protegiendo la privacidad de las interacciones virtuales.
EGRESADOS	Mantener disponible los registros de notas y constancias de egreso de la institución.	Tener acceso a los registros de notas y constancias de egreso de la institución de manera oportuna y de forma rápida.
PROVEEDORES	Cumplimiento de obligaciones pactadas.	Administración de los contratos de manera transparente y efectiva.
VISITANTES	Excelencia en el servicio.	Atención rápida, oportuna y de manera efectiva.
ORGANISMOS GUBERNAMENTALES APLICABLES	Excelencia en el servicio.	Atención rápida, oportuna y de manera efectiva.
OTRAS INSTITUCIONES EDUCATIVAS	Alianzas para desarrollar acciones colaborativas.	Beneficios mutuos.

Nota: Elaboración Propia

A.3. ALCANCES Y LIMITACIONES

TABLA VII ALCANCES Y LIMITACIONES

ALCANCES	DESCRIPCIÓN
El SGSI abarcará los principales procesos de la institución	Se tomará en cuenta los procesos core de la Institución educativa, abarcando el área administrativa y los salones de innovación y EPT donde se centra la mayor cantidad de equipos tecnológicos.
Protección de información sensible del personal y estudiantes	El SGSI se centrará en la protección de la información personal y sensible de docentes, personal administrativo y estudiantes, incluyendo datos académicos y personales.
Implementación de Controles de Acceso	Se establecerán controles de acceso adecuados para garantizar que la información esté disponible solo para personas autorizadas, asegurando la confidencialidad e integridad de los datos.
Respuesta Efectiva a Incidentes de Seguridad	Se establecerá un plan de respuesta a incidentes para abordar de manera efectiva cualquier violación de seguridad, minimizando el impacto y restaurando la operatividad normal lo antes posible.
Programas de Concientización y Capacitación:	Se desarrollarán programas de concientización y capacitación para educar al personal, docentes y estudiantes sobre las mejores prácticas de seguridad de la información, fomentando una cultura de seguridad.
LIMITACIONES	
DESCRIPCIÓN	**IMPACTO**
Restricciones presupuestarias para la implementación y mantenimiento efectivo de un sistema de gestión de la seguridad de la información	La falta de inversión podría afectar la adquisición de herramientas de seguridad, la formación del personal y la implementación de controles adecuados.
falta de conciencia y comprensión sobre la importancia de la seguridad de la información entre el personal, docentes y estudiantes.	La resistencia al cambio y la falta de adhesión a las políticas de seguridad podrían comprometer la efectividad del SGSI.

Carencia de personal capacitado en seguridad de la información, lo que dificulta la implementación y gestión adecuada del SGSI.	La falta de expertos en seguridad podría conducir a una respuesta ineficiente ante incidentes y a una gestión inadecuada de riesgos.
La infraestructura tecnológica del colegio es obsoleta, lo que dificulta la implementación de controles de seguridad actualizados y eficaces.	Las vulnerabilidades inherentes a sistemas obsoletos podrían exponer la información a riesgos de seguridad, y la actualización puede requerir inversiones significativas.
La cultura organizacional del colegio puede no favorecer la transparencia, la comunicación abierta o la colaboración, lo que complica la implementación de un SGSI basado en la participación de todos los miembros.	La falta de una cultura de seguridad podría dar lugar a la falta de colaboración en la identificación y gestión de riesgos, así como a una respuesta inadecuada a incidentes.

Nota: Elaboración Propia, en base a los datos recopilados de la Institución Educativa.

B. LIDERAZGO

B.1. LÍDERES Y RESPONSABILIDADES

TABLA VIII LÍDERES Y RESPONSABILIDADES

ROL	RESPONSABILIDADES
JEFE DE PROYECTO	- Conocer a profundidad la organización de la institución educativa (visión, misión, organigrama institucional, roles y funciones de los miembros de la comunidad educativa, alcances y limitaciones).
	- Elaborar el adecuado inventario de activos críticos de la I.E.
	- Elaborar un cuadro con las amenazas y vulnerabilidades de los respectivos activos.
	- Elaborar las políticas de seguridad y procedimientos.
	- Colaborar en la implementación de los controles de acceso respectivos.
	- Elaborar el plan de concientización y capacitación sobre seguridad de la información.

DIRECTOR	- Establecer la visión y el compromiso con la seguridad de la información en toda la institución.
	- Garantizar la asignación de recursos necesarios para implementar y mantener el SGSI.
	- Revisar y aprobar políticas de seguridad y procedimientos.
	- Comunicar la importancia de la seguridad a todo el personal y estudiantes.
DOCENTES	- Proteger la confidencialidad de la información estudiantil.
	- Seguir los procedimientos de seguridad al manejar documentos y datos sensibles.
	- Participar en programas de concientización y capacitación sobre seguridad.
	- Informar de posibles riesgos o incidentes de seguridad al jefe de proyecto
COORDINADORES ACADÉMICOS	- Garantizar la seguridad de la información en sus respectivas áreas académicas.
	- Colaborar en la identificación y evaluación de riesgos específicos del área académica.
	- Implementar procedimientos de seguridad en la gestión de información académica.
	- Participar activamente en la mejora continua del SGSI en su área.
COORDINADOR DE INNOVACIÓN Y SOPORTE TECNOLÓGICO (CIST)	- Mantener actualizado y seguro el software y hardware de la institución.
	- Implementar y gestionar controles de acceso a los sistemas informáticos.
	- Monitorear y responder a incidentes de seguridad relacionados con la tecnología.
	- Colaborar con el personal docente para garantizar la seguridad de la información.
	- Colaborar en la implementación de medidas físicas de seguridad.

PERSONAL DE VIGILANCIA	- Reportar cualquier actividad sospechosa o violación de seguridad.
	- Participar en simulacros de seguridad y procedimientos de evacuación.
	- Colaborar con el jefe de proyecto en la implementación de medidas preventivas.
SECRETARIA	- Manejar y proteger la información confidencial y sensible de la institución.
	- Aplicar controles de acceso físicos a la documentación importante.
	- Colaborar en la elaboración y actualización de políticas de seguridad de la información.
	- Participar en programas de concientización y capacitación sobre seguridad.
AUXILIAR DE EDUCACIÓN	- Colaborar en la supervisión y aplicación de medidas de seguridad en el entorno escolar.
	- Participar en simulacros de seguridad y procedimientos de evacuación.
	- Colaborar con el personal docente y de vigilancia en la implementación de medidas preventivas.
	- Reportar posibles riesgos o incidentes de seguridad al jefe de proyecto.
ESTUDIANTES	- Proteger la confidencialidad de su propia información personal y académica.
	- Seguir las normas y políticas de seguridad establecidas por la institución.
	- Participar en programas de concientización sobre seguridad de la información.
	- Reportar incidentes de seguridad o violaciones a un adulto responsable.

Nota: Elaboración Propia, con apoyo de la comunidad educativa.

C. PLANEACIÓN

C.1. ACCIONES PARA ABORDAR RIESGOS Y OPORTUNIDADES

TABLA IX ACCIONES PARA ABORDAR RIESGOS Y OPORTUNIDADES

ACTIVO	AMENAZA	VULNERABILIDAD	PROPIETARIO DEL RIESGO
AMPLIFICADOR DE AUDIO	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DIRECTOR
	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	
	Polvo	Falta de limpieza constante del equipo	
	Fallas en los equipos	No existe reemplazo inmediato del equipo	
	Corte de energía	No existe UPS	
	Error de configuración	No existe manual de uso	
	Error de mant. de hardware	No existe manual de uso	
	Pérdida del equipo	El equipo es prestado a cualquier usuario que lo necesite	
		Falta de medidas de seguridad física	
	Insertar virus o malware	Falta de programas antivirus	
		Descarga de software no seguras	
	Robo del equipo	Lugar de almacenamiento poco seguro	
ARCHIVADOR DE MADERA	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DIRECTOR
	Polvo	Falta de limpieza constante del equipo	
	Pérdida	Falta de medidas de seguridad física	
	Robo	Lugar de almacenamiento poco seguro	
	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	

ARCHIVADOR DE METAL	Polvo	Falta de limpieza constante del equipo	PERSONAL DE VIGILANCIA
	Pérdida	Falta de medidas de seguridad física	
	Robo	Lugar de almacenamiento poco seguro	
ARMARIO DE METAL	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DOCENTE ASIGNADO
	Polvo	Falta de limpieza constante del equipo	
	Pérdida	Falta de medidas de seguridad física	
	Robo	Puerta de acceso siempre abierta	
ARMARIO DE METAL	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	CIST
	Polvo	Falta de limpieza constante del equipo	
	Pérdida	Falta de medidas de seguridad física	
	Robo	Puerta de acceso con cerradura sin funcionar	
COMPUTADORA PERSONAL PORTÁTIL DE DIRECCIÓN	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DIRECTOR
	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	
	Polvo	Falta de limpieza constante del equipo	
	Fallas en los equipos	No existe reemplazo inmediato del equipo	
	Corte de energía	No existe UPS	
		Batería malograda, funciona siempre conectado a la energía	
	Error de administrador	Falta de software administrador de núcleo (protección de partituras del disco)	
		Contraseña de inicio de sesión inexistente	
	Error de configuración	Falta de software administrador de núcleo (protección de partituras del disco)	

	Error de usuario	Falta de software administrador de núcleo (protección de partituras del disco)	
	Aparición de virus o malware	Falta de programas antivirus/antimalware	
		Descargas de software no seguras.	
	Sobrecalentamiento	Batería malograda, funciona siempre conectado a la energía	
	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	
	Error de actualización de Software	Descargas de software no seguras.	
		Software obsoleto	
	Error de mantenimiento de Software	Manual de usuario no disponible	
		Desconocimiento del usuario	
	Error de mantenimiento de Hardware	Manual de usuario no disponible	
		Desconocimiento del usuario	
	Manipulación de configuraciones	Falta de software administrador de núcleo (protección de partituras del disco)	
		Contraseña de inicio de sesión inexistente	
	Insertar virus o malware	Falta de programas antivirus/antimalware	
	Acceso sin autorización	Contraseña de inicio de sesión inexistente	
	Eliminación de información digital	Falta de copias de seguridad	
		Contraseña de inicio de sesión inexistente	
	Robo de equipos	Falta de medidas de seguridad física	

COMPUTADORA PERSONAL PORTÁTIL DE DOCENTE	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DOCENTE ASIGNADO
	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	
	Polvo	Falta de limpieza constante del equipo	
	Fallas en los equipos	No existe reemplazo inmediato del equipo	
	Corte de energía	No existe UPS	
		Batería malograda, funciona siempre conectado a la energía	
	Error de administrador	Falta de software administrador de núcleo (protección de partituras del disco)	
		Contraseña de inicio de sesión inexistente	
	Error de configuración	Falta de software administrador de núcleo (protección de partituras del disco)	
	Error de usuario	Falta de software administrador de núcleo (protección de partituras del disco)	
	Aparición de virus o malware	Falta de programas antivirus/antimalware	
		Descargas de software no seguras.	
	Sobrecalentamiento	Batería malograda, funciona siempre conectado a la energía	
	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	
	Error de actualización de Software	Descargas de software no seguras.	
		Software obsoleto	
	Error de mantenimiento de Software	Manual de usuario no disponible	
		Desconocimiento del usuario	
		Manual de usuario no disponible	

	Error de mantenimiento de Hardware	Desconocimiento del usuario	
	Manipulación de configuraciones	Falta de software administrador de núcleo (protección de partituras del disco)	
		Contraseña de inicio de sesión inexistente	
	Insertar virus o malware	Falta de programas antivirus/antimalware	
	Acceso sin autorización	Contraseña de inicio de sesión inexistente	
	Eliminación de información digital	Falta de copias de seguridad	
		Contraseña de inicio de sesión inexistente	
	Robo de equipos	Falta de medidas de seguridad física	
COMPUTADORA PERSONAL PORTÁTIL DE ESTUDIANTE	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	CIST
	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	
	Polvo	Falta de limpieza constante del equipo	
	Fallas en los equipos	No existe reemplazo inmediato del equipo	
	Corte de energía	No existe UPS	
		Batería malograda, funciona siempre conectado a la energía	
	Error de administrador	Falta de software administrador de núcleo (protección de partituras del disco)	
		Contraseña de inicio de sesión visible en la web	
	Error de configuración	Falta de software administrador de núcleo (protección de partituras del disco)	
	Error de usuario	Falta de software administrador de núcleo (protección de partituras del disco)	

	Aparición de virus o malware	Falta de programas antivirus/antimalware	
		Descargas de software no seguras.	
	Sobrecalentamiento	Batería malograda, funciona siempre conectado a la energía	
	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	
	Error de actualización de Software	Descargas de software no seguras.	
		Software obsoleto	
	Error de mantenimiento de Software	Manual de usuario no disponible	
		Desconocimiento del usuario	
	Error de mantenimiento de Hardware	Manual de usuario no disponible	
		Desconocimiento del usuario	
	Manipulación de configuraciones	Falta de software administrador de núcleo (protección de partituras del disco)	
		Contraseña de inicio de sesión visibles en la web	
	Insertar virus o malware	Falta de programas antivirus/antimalware	
	Acceso sin autorización	Contraseña de inicio de sesión visible en la web	
	Eliminación de información digital	Falta de copias de seguridad	
		Contraseña de inicio de sesión débil	
	Robo de equipos	Falta de medidas de seguridad física	

COMPUTADORA PERSONAL PORTÁTIL ALMACENADA	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	PERSONAL DE VIGILANCIA
	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	
	Polvo	Falta de limpieza constante del equipo	
	Fallas en los equipos	No existe reemplazo inmediato del equipo	
	Corte de energía	No existe UPS	
		Batería malograda, funciona siempre conectado a la energía	
	Error de administrador	Falta de software administrador de núcleo (protección de partituras del disco)	
		Contraseña de inicio de sesión inexistente	
	Error de configuración	Falta de software administrador de núcleo (protección de partituras del disco)	
	Error de usuario	Falta de software administrador de núcleo (protección de partituras del disco)	
	Aparición de virus o malware	Falta de programas antivirus/antimalware	
		Descargas de software no seguras.	
	Sobrecalentamiento	Batería malograda, funciona siempre conectado a la energía	
	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	
	Error de actualización de Software	Descargas de software no seguras.	
		Software obsoleto	
	Error de mantenimiento de Software	Manual de usuario no disponible	
		Desconocimiento del usuario	
		Manual de usuario no disponible	

	Error de mantenimiento de Hardware	Desconocimiento del usuario	
	Manipulación de configuraciones	Falta de software administrador de núcleo (protección de partituras del disco)	
		Contraseña de inicio de sesión inexistente	
	Insertar virus o malware	Falta de programas antivirus/antimalware	
	Acceso sin autorización	Contraseña de inicio de sesión inexistente	
	Eliminación de información digital	Falta de copias de seguridad	
		Contraseña de inicio de sesión inexistente	
	Robo de equipos	Falta de medidas de seguridad física	
CONSOLA PARA CONTROL DE AUDIO	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	PERSONAL DE VIGILANCIA
	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	
	Polvo	Falta de limpieza constante del equipo	
	Fallas en los equipos	No existe reemplazo inmediato del equipo	
	Corte de energía	No existe UPS	
DISCO DURO EXTERNO	Error de configuración	No existe manual de usuario	CIST
	Error de usuario	Descarga de programas de dudosa procedencia	
	Aparición de virus o malware	Falta de programas antivirus/antimalware	
		Descargas de software no seguras.	
	Sobrecalentamiento	Uso excesivo del equipo	
	Borrar información	No existe copias de respaldo	
	Pérdida	No existe control de préstamo	
	Robo	No existe lugar seguro de almacenamiento	

EQUIPO DE SONIDO	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	CIST
	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	
	Polvo	Falta de limpieza constante del equipo	
	Fallas en los equipos	No existe reemplazo inmediato del equipo	
	Corte de energía	No existe UPS	
	Robo	Cerradura de puerta no sirve	
	Pérdida	No existe control de préstamo	
ESTABILIZADOR	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DIRECTOR
	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	
	Polvo	Falta de limpieza constante del equipo	
	Fallas en los equipos	No existe reemplazo inmediato del equipo	
	Corte de energía	No existe UPS	
	Robo	Falta de controles físicos	
FOTOCOPIADORA EN GENERAL	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DIRECTOR
	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	
	Polvo	Falta de limpieza constante del equipo	
	Fallas en los equipos	No existe reemplazo inmediato del equipo	
	Corte de energía	No existe UPS	
	Error de configuración	No existe manual de usuario	
	Error de usuario	Desconocimiento de uso	
	Acceso sin autorización	Cualquier usuario puede utilizarlo sin permiso	

IMPRESORAS	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DIRECTOR
	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	
	Polvo	Falta de limpieza constante del equipo	
	Fallas en los equipos	No existe reemplazo inmediato del equipo	
	Corte de energía	No existe UPS	
	Error de configuración	Manual de usuario almacenado en otro lugar	
	Error de usuario	Desconocimiento de uso	
REPRODUCTOR DE VIDEO	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	DIRECTOR
	Fallas en los equipos	No existe reemplazo inmediato del equipo	
	Corte de energía	No existe UPS	
	Error de usuario	Manipulación inadecuada	
SERVIDOR	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	CIST
	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	
	Polvo	Falta de limpieza constante del equipo	
	Fallas en los equipos	No existe reemplazo inmediato del equipo	
	Corte de energía	No existe UPS	
	Error de usuario	Manipulación inadecuada	
PROYECTOR MULTIMEDIA	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DOCENTE ASIGNADO
	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	
	Fallas en los equipos	No existe reemplazo inmediato del equipo	
	Corte de energía	No existe UPS	
	Error de usuario	Manipulación inadecuada	
		Manual de usuario no disponible	

	Error de mantenimiento de Hardware	Desconocimiento del usuario	
		Mal uso del lente óptico	
	Robo	Puertas de acceso siempre abiertas	
TELEVISOR LED	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DOCENTE ASIGNADO
	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	
	Fallas en los equipos	No existe reemplazo inmediato del equipo	
	Corte de energía	No existe UPS	
	Error de usuario	Manipulación inadecuada	
	Error de mantenimiento de Hardware	Uso de implementos de limpieza inadecuados	
	Robo	Puertas de acceso siempre abiertas	
UNIDAD CENTRAL DE PROCESO - CPU	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	SECRETARIA
	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	
	Polvo	Falta de limpieza constante del equipo	
	Fallas en los equipos	No existe reemplazo inmediato del equipo	
	Corte de energía	No existe UPS	
	Error de administrador	Falta de software administrador de núcleo (protección de partituras del disco)	
		Contraseña de inicio de sesión inexistente	
	Error de configuración	Falta de software administrador de núcleo (protección de partituras del disco)	
	Error de usuario	Falta de software administrador de núcleo (protección de partituras del disco)	

	Aparición de virus o malware	Falta de programas antivirus/antimalware	
		Descargas de software no seguras.	
	Sobrecalentamiento	Batería malograda, funciona siempre conectado a la energía	
	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	
	Error de actualización de Software	Descargas de software no seguras.	
		Software obsoleto	
	Error de mantenimiento de Software	Manual de usuario inexistente	
		Desconocimiento del usuario	
	Error de mantenimiento de Hardware	Desconocimiento del usuario	
	Exceso de confianza	El personal confía sus claves a personal de confianza	
	Manipulación de configuraciones	Falta de software administrador de núcleo (protección de partituras del disco)	
		Contraseña de inicio de sesión inexistente	
	Insertar virus o malware	Falta de programas antivirus/antimalware	
	Acceso sin autorización	Contraseña de inicio de sesión inexistente	
	Eliminación de información digital	Falta de copias de seguridad	
		Contraseña de inicio de sesión inexistente	
	Robo de equipos	Falta de medidas de seguridad física	
CÁMARA DE VIGILANCIA	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	DIRECTOR
	Polvo	Falta de limpieza constante del equipo	
	Fallas en los equipos	No existe reemplazo inmediato del equipo	

	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	
	Error de actualización de Software	Software obsoleto	
	Acceso sin autorización	Contraseña de inicio de sesión inexistente	
	Eliminación de información digital	Falta de copias de seguridad	
		Contraseña de inicio de sesión inexistente	
	Robo de equipos	Falta de medidas de seguridad física	
LIBRO DE INCIDENCIAS	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DIRECTOR
	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	
	Borrar información	Falta de copias de seguridad	
	Robo o pérdida	Pocos o nulos controles de acceso	
	Suplantación de identidad	Falta de políticas de autenticación	
CUADERNO DE ATENCIONES	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	COORDINADOR DE TUTORÍA
	Borrar información	Falta de copias de seguridad	
	Robo o pérdida	Pocos o nulos controles de acceso	
	Suplantación de identidad	Falta de políticas de autenticación	
CUADERNO DE INCIDENCIAS	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	PSICÓLOGO
	Borrar información	Falta de copias de seguridad	
	Robo o pérdida	Pocos o nulos controles de acceso	

	Suplantación de identidad	Falta de políticas de autenticación	
ACTA DE EVALUACIÓN Y CERTIFICADO DE ESTUDIOS	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DIRECTOR
	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	
	Borrar información	Falta de copias de seguridad	
	Robo o pérdida	Pocos o nulos controles de acceso	
FICHAS DE MONITOREO CIENCIAS	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	COORDINADOR DE CIENCIAS
	Borrar información	Falta de copias de seguridad	
	Robo o pérdida	Pocos o nulos controles de acceso	
	Suplantación de identidad	Falta de políticas de autenticación	
FICHAS DE MONITOREO LETRAS	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	COORDINADOR DE LETRAS
	Borrar información	Falta de copias de seguridad	
	Robo o pérdida	Pocos o nulos controles de acceso	
	Suplantación de identidad	Falta de políticas de autenticación	
REG. DE ASISTENCIA TRABAJADORES	Borrar información	Falta de copias de seguridad	DIRECTOR
	Robo o pérdida	Pocos o nulos controles de acceso	
REG. DE ASISTENCIA ESTUDIANTES	Borrar información	Falta de copias de seguridad	AUXILIAR
	Robo o pérdida	Pocos o nulos controles de acceso	

MEMORÁNDUMS	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	DIRECTOR
	Borrar información	Falta de copias de seguridad	
	Robo o pérdida	Pocos o nulos controles de acceso	
	Suplantación de identidad	Falta de políticas de autenticación	
BOLETA DE NOTAS	Borrar información	Falta de copias de seguridad	DIRECTOR
	Robo o pérdida	Pocos o nulos controles de acceso	
CONTRASEÑAS DE EQUIPOS	Error de configuración	Configuración poco segura puede ser explotada	CIST
	Ingeniería social	Desconocimiento del personal a diferentes tipos de ataques	
	Exceso de confianza	El personal confía sus claves a personal de confianza	
REGLAMENTO INTERNO INSTITUCIONAL	Borrar información	Falta de copias de seguridad	DIRECTOR
	Robo o pérdida	Pocos o nulos controles de acceso	
PLAN ANUAL DE TRABAJO	Borrar información	Falta de copias de seguridad	DIRECTOR
	Robo o pérdida	Pocos o nulos controles de acceso	
PROYECTO EDUCATIVO INSTITUCIONAL	Borrar información	Falta de copias de seguridad	DIRECTOR
	Robo o pérdida	Pocos o nulos controles de acceso	
SISTEMA OPERATIVO WIN10	Error de configuración	Configuración predeterminada no óptima para los equipos	CIST
	Error de administración	Débil gestión de contraseñas	
	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	
		Falta de programas antivirus/antimalware	

	Aparición de virus o malware	Descargas de software no seguras.	
	Licencia ilegal de software	Ataques de tipo rasomware	
SISTEMA OPERATIVO WIN8 PRO	Error de configuración	Configuración predeterminada no óptima para los equipos	CIST
	Error de administración	Débil gestión de contraseñas	
	Error de actualización de Software	Software desfasado para la actualidad	
	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	
	Aparición de virus o malware	Falta de programas antivirus/antimalware	
		Descargas de software no seguras.	
	Licencia ilegal de software	Ataques de tipo rasomware	
MICROSOFT OFFICE 2013	Error de configuración	Configuración predeterminada no óptima para los equipos	CIST
	Error de actualización de Software	Software desfasado para la actualidad	
	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	
	Licencia ilegal de software	Ataques de tipo rasomware	
MICROSOFT OFFICE 2016	Error de configuración	Configuración predeterminada no óptima para los equipos	CIST
	Error de actualización de Software	Software desfasado para la actualidad	
	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	

	Licencia ilegal de software	Ataques de tipo rasomware	
SCRATCH V3	Error de configuración	Configuración predeterminada no óptima para los equipos	CIST
	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	
XMIND	Error de configuración	Configuración predeterminada no óptima para los equipos	CIST
	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	
CMAPTOOLS	Error de configuración	Configuración predeterminada no óptima para los equipos	CIST
	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	
MODEM ROUTER	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DIRECTOR
	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	
	Polvo	Falta de limpieza constante del equipo	
	Fallas en los equipos	No existe reemplazo inmediato del equipo	
	Corte de energía	No existe UPS	
	Error de usuario	Manipulación inadecuada	

Nota: Descripción del activo crítico sus principales amenazas y vulnerabilidades.

2. HACER

A.1. EVALUACIÓN DE RIESGOS DE SEGURIDAD

A.1.1. GESTIÓN DE RIESGOS

Metodología

TABLA X. METODOLOGÍA DE GESTIÓN DE RIESGOS.

MATRIZ DE RIESGOS I.E. FRANCISCO DE ZELA			IMPACTO				
			Mínima	Baja	Moderada	Mayor	Máxima
			1	2	3	4	5
PROBABILIDAD	Muy Alta	5	5	10	15	20	25
	alta	4	4	8	12	16	20
	Media	3	3	6	9	12	15
	Baja	2	2	4	6	8	10
	Muy Baja	1	1	2	3	4	5

Nota: Elaboración Propia, en base a la estimación de la comunidad educativa.

TABLA XI. NIVEL DE RIESGO.

Nivel de riesgo			
Mínimo	máximo	Nivel	color
1	4	Aceptable	
5	10	Tolerable	
11	15	Alto	
16	25	Extremo	

Nota:: Elaboración Propia, en base a la estimación de la comunidad educativa

Análisis

TABLA XII. ANÁLISIS DE RIESGOS.

ACTIVO	ID DE RIESGO	AMENAZA	VULNERABILIDAD	PROPIETARIO DEL RIESGO	IMPACTO	PROBABILIDAD	RIESGO
AMPLIFICADOR DE AUDIO	RFZ01	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DIRECTOR	5	1	5
	RFZ02	Rayo	No existe un pararrayos que proteja ante descargas eléctricas		4	1	4
	RFZ03	Polvo	Falta de limpieza constante del equipo		3	3	9
	RFZ04	Fallas en los equipos	No existe reemplazo inmediato del equipo		5	3	15
	RFZ05	Corte de energía	No existe UPS		4	2	8
	RFZ06	Error de configuración	No existe manual de uso		4	2	8
	RFZ07	Error de mantenimiento de hardware	No existe manual de uso		4	2	8
	RFZ08	Pérdida del equipo	El equipo es prestado a cualquier usuario que lo necesite		5	3	15
	RFZ09		Falta de medidas de seguridad física		5	4	20
	RFZ10	Insertar virus o malware	Falta de programas antivirus		4	3	12
	RFZ11		Descarga de software no seguras		4	3	12
	RFZ12	Robo del equipo	Lugar de almacenamiento poco seguro		5	3	15
ARCHIVADOR DE MADERA	RFZ13	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DIRECTOR	5	1	5
	RFZ14	Polvo	Falta de limpieza constante del equipo		3	1	3
	RFZ15	Pérdida	Falta de medidas de seguridad física		5	2	10
	RFZ16	Robo	Lugar de almacenamiento poco seguro		5	3	15

ARCHIVADOR DE METAL	RFZ17	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	PERSONAL DE VIGILANCIA	5	1	5
	RFZ18	Polvo	Falta de limpieza constante del equipo		3	2	6
	RFZ19	Pérdida	Falta de medidas de seguridad física		5	3	15
	RFZ20	Robo	Lugar de almacenamiento poco seguro		5	3	15
ARMARIO DE METAL	RFZ21	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DOCENTE ASIGNADO	5	1	5
	RFZ22	Polvo	Falta de limpieza constante del equipo		3	2	6
	RFZ23	Pérdida	Falta de medidas de seguridad física		5	3	15
	RFZ24	Robo	Puerta de acceso siempre abierta		5	3	15
ARMARIO DE METAL	RFZ25	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	CIST	5	1	5
	RFZ26	Polvo	Falta de limpieza constante del equipo		3	2	6
	RFZ27	Pérdida	Falta de medidas de seguridad física		5	3	15
	RFZ28	Robo	Puerta de acceso con cerradura sin funcionar		5	3	15
COMPUTADORA PERSONAL PORTÁTIL DE DIRECCIÓN	RFZ29	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DIRECTOR	5	1	5
	RFZ30	Rayo	No existe un pararrayos que proteja ante descargas eléctricas		4	1	4
	RFZ31	Polvo	Falta de limpieza constante del equipo		3	3	9
	RFZ32	Fallas en los equipos	No existe reemplazo inmediato del equipo		4	3	12
	RFZ33	Corte de energía	No existe UPS		4	2	8
	RFZ34		Batería malograda, funciona siempre conectado a la energía		4	2	8
	RFZ35	Error de administrador	Falta de software administrador de núcleo (protección de partituras del disco)		3	3	9
	RFZ36		Contraseña de inicio de sesión inexistente		4	4	16

	RFZ37	Error de configuración	Falta de software administrador de núcleo (protección de partituras del disco)		3	3	9
	RFZ38	Error de usuario	Falta de software administrador de núcleo (protección de partituras del disco)		4	3	12
	RFZ39	Aparición de virus o malware	Falta de programas antivirus/antimalware		4	3	12
	RFZ40		Descargas de software no seguras.		4	4	16
	RFZ41	Sobrecalentamiento	Batería malograda, funciona siempre conectado a la energía		3	3	9
	RFZ42	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)		5	4	20
	RFZ43	Error de actualización de Software	Descargas de software no seguras.		4	3	12
	RFZ44		Software obsoleto		3	3	9
	RFZ45	Error de mantenimiento de Software	Manual de usuario no disponible		3	2	6
	RFZ46		Desconocimiento del usuario		3	2	6
	RFZ47	Error de mantenimiento de Hardware	Manual de usuario no disponible		3	1	3
	RFZ48		Desconocimiento del usuario		3	3	9
	RFZ49	Manipulación de configuraciones	Falta de software administrador de núcleo (protección de partituras del disco)		2	2	4
	RFZ50		Contraseña de inicio de sesión inexistente		5	3	15
	RFZ51	Insertar virus o malware	Falta de programas antivirus/antimalware		4	3	12
	RFZ52	Acceso sin autorización	Contraseña de inicio de sesión inexistente		4	4	16
	RFZ53	Eliminación de información digital	Falta de copias de seguridad		5	3	15
	RFZ54		Contraseña de inicio de sesión inexistente		5	5	25
	RFZ55	Robo de equipos	Falta de medidas de seguridad física		5	3	15

COMPUTADORA PERSONAL PORTÁTIL DE DOCENTE	RFZ56	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DOCENTE ASIGNADO	5	3	15
	RFZ57	Rayo	No existe un pararrayos que proteja ante descargas eléctricas		4	3	12
	RFZ58	Polvo	Falta de limpieza constante del equipo		3	3	9
	RFZ59	Fallas en los equipos	No existe reemplazo inmediato del equipo		4	3	12
	RFZ60	Corte de energía	No existe UPS		4	3	12
	RFZ61		Batería malograda, funciona siempre conectado a la energía		4	3	12
	RFZ62	Error de administrador	Falta de software administrador de núcleo (protección de partituras del disco)		3	3	9
	RFZ63		Contraseña de inicio de sesión inexistente		4	4	16
	RFZ64	Error de configuración	Falta de software administrador de núcleo (protección de partituras del disco)		3	3	9
	RFZ65	Error de usuario	Falta de software administrador de núcleo (protección de partituras del disco)		4	3	12
	RFZ66	Aparición de virus o malware	Falta de programas antivirus/antimalware		4	3	12
	RFZ67		Descargas de software no seguras.		4	4	16
	RFZ68	Sobrecalentamiento	Batería malograda, funciona siempre conectado a la energía		3	3	9
	RFZ69	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)		5	4	20
	RFZ70	Error de actualización de Software	Descargas de software no seguras.		4	3	12
	RFZ71		Software obsoleto		3	3	9
	RFZ72	Error de mantenimiento de Software	Manual de usuario no disponible		3	2	6
	RFZ73		Desconocimiento del usuario		3	2	6
	RFZ74	Error de mantenimiento de Hardware	Manual de usuario no disponible		3	1	3
	RFZ75		Desconocimiento del usuario		3	3	9

	RFZ76	Manipulación de configuraciones	Falta de software administrador de núcleo (protección de partituras del disco)		2	2	4
	RFZ77		Contraseña de inicio de sesión inexistente		5	3	15
	RFZ78	Insertar virus o malware	Falta de programas antivirus/antimalware		4	3	12
	RFZ79	Acceso sin autorización	Contraseña de inicio de sesión inexistente		4	4	16
	RFZ80	Eliminación de información digital	Falta de copias de seguridad		5	3	15
	RFZ81		Contraseña de inicio de sesión inexistente		5	5	25
	RFZ82	Robo de equipos	Falta de medidas de seguridad física		5	3	15
COMPUTADORA PERSONAL PORTÁTIL DE ESTUDIANTE	RFZ83	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	CIST	5	3	15
	RFZ84	Rayo	No existe un pararrayos que proteja ante descargas eléctricas		4	3	12
	RFZ85	Polvo	Falta de limpieza constante del equipo		3	3	9
	RFZ86	Fallas en los equipos	No existe reemplazo inmediato del equipo		4	3	12
	RFZ87	Corte de energía	No existe UPS		4	3	12
	RFZ88		Batería malograda, funciona siempre conectado a la energía		4	3	12
	RFZ89	Error de administrador	Falta de software administrador de núcleo (protección de partituras del disco)		3	3	9
	RFZ90		Contraseña de inicio de sesión visible en la web		4	4	16
	RFZ91	Error de configuración	Falta de software administrador de núcleo (protección de partituras del disco)		3	3	9
	RFZ92	Error de usuario	Falta de software administrador de núcleo (protección de partituras del disco)		4	3	12
	RFZ93	Aparición de virus o malware	Falta de programas antivirus/antimalware		4	3	12
	RFZ94		Descargas de software no seguras.		4	4	16

	RFZ95	Sobrecalentamiento	Batería malograda, funciona siempre conectado a la energía		3	3	9
	RFZ96	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)		5	4	20
	RFZ97	Error de actualización de Software	Descargas de software no seguras.		4	3	12
	RFZ98		Software obsoleto		3	3	9
	RFZ99	Error de mantenimiento de Software	Manual de usuario no disponible		3	2	6
	RFZ100		Desconocimiento del usuario		3	2	6
	RFZ101	Error de mantenimiento de Hardware	Manual de usuario no disponible		3	1	3
	RFZ102		Desconocimiento del usuario		3	3	9
	RFZ103	Manipulación de configuraciones	Falta de software administrador de núcleo (protección de partituras del disco)		2	2	4
	RFZ104		Contraseña de inicio de sesión visibles en la web		5	3	15
	RFZ105	Insertar virus o malware	Falta de programas antivirus/antimalware		4	3	12
	RFZ106	Acceso sin autorización	Contraseña de inicio de sesión visible en la web		4	4	16
	RFZ107	Eliminación de información digital	Falta de copias de seguridad		5	3	15
	RFZ108		Contraseña de inicio de sesión débil		5	5	25
	RFZ109	Robo de equipos	Falta de medidas de seguridad física		5	3	15
COMPUTADORA PERSONAL PORTÁTIL ALMACENADA	RFZ110	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	PERSONAL DE VIGILANCIA	5	3	15
	RFZ111	Rayo	No existe un pararrayos que proteja ante descargas eléctricas		4	3	12
	RFZ112	Polvo	Falta de limpieza constante del equipo		3	3	9
	RFZ113	Fallas en los equipos	No existe reemplazo inmediato del equipo		4	3	12
	RFZ114		No existe UPS		4	3	12

	RFZ115	Corte de energía	Batería malograda, funciona siempre conectado a la energía		4	3	12
	RFZ116	Error de administrador	Falta de software administrador de núcleo (protección de partituras del disco)		3	3	9
	RFZ117		Contraseña de inicio de sesión inexistente		4	4	16
	RFZ118	Error de configuración	Falta de software administrador de núcleo (protección de partituras del disco)		3	3	9
	RFZ119	Error de usuario	Falta de software administrador de núcleo (protección de partituras del disco)		4	3	12
	RFZ120	Aparición de virus o malware	Falta de programas antivirus/antimalware		4	3	12
	RFZ121		Descargas de software no seguras.		4	4	16
	RFZ122	Sobrecalentamiento	Batería malograda, funciona siempre conectado a la energía		3	3	9
	RFZ123	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)		5	4	20
	RFZ124	Error de actualización de Software	Descargas de software no seguras.		4	3	12
	RFZ125		Software obsoleto		3	3	9
	RFZ126	Error de mantenimiento de Software	Manual de usuario no disponible		3	2	6
	RFZ127		Desconocimiento del usuario		3	2	6
	RFZ128	Error de mantenimiento de Hardware	Manual de usuario no disponible		3	1	3
	RFZ129		Desconocimiento del usuario		3	3	9
	RFZ130	Manipulación de configuraciones	Falta de software administrador de núcleo (protección de partituras del disco)		2	2	4
	RFZ131		Contraseña de inicio de sesión inexistente		5	3	15
	RFZ132	Insertar virus o malware	Falta de programas antivirus/antimalware		4	3	12
	RFZ133	Acceso sin autorización	Contraseña de inicio de sesión inexistente		4	4	16

	RFZ134	Eliminación de información digital	Falta de copias de seguridad		5	3	15
	RFZ135		Contraseña de inicio de sesión inexistente		5	5	25
	RFZ136	Robo de equipos	Falta de medidas de seguridad física		5	3	15
CONSOLA PARA CONTROL DE AUDIO	RFZ137	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	PERSONAL DE VIGILANCIA	4	2	8
	RFZ138	Rayo	No existe un pararrayos que proteja ante descargas eléctricas		4	2	8
	RFZ139	Polvo	Falta de limpieza constante del equipo		3	2	6
	RFZ140	Fallas en los equipos	No existe reemplazo inmediato del equipo		4	3	12
	RFZ141	Corte de energía	No existe UPS		4	4	16
DISCO DURO EXTERNO	RFZ142	Error de configuración	No existe manual de usuario	CIST	2	2	4
	RFZ143	Error de usuario	Descarga de programas de dudosa procedencia		4	3	12
	RFZ144	Aparición de virus o malware	Falta de programas antivirus/antimalware		4	4	16
	RFZ145		Descargas de software no seguras.		4	4	16
	RFZ146	Sobrecalentamiento	Uso excesivo del equipo		4	1	4
	RFZ147	Borrar información	No existe copias de respaldo		4	2	8
	RFZ148	Pérdida	No existe control de préstamo		4	3	12
	RFZ149	Robo	No existe lugar seguro de almacenamiento		5	2	10

EQUIPO DE SONIDO	RFZ150	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	CIST	4	1	4
	RFZ151	Rayo	No existe un pararrayos que proteja ante descargas eléctricas		3	2	6
	RFZ152	Polvo	Falta de limpieza constante del equipo		2	2	4
	RFZ153	Fallas en los equipos	No existe reemplazo inmediato del equipo		4	4	16
	RFZ154	Corte de energía	No existe UPS		4	3	12
	RFZ155	Robo	Cerradura de puerta no sirve		5	5	25
	RFZ156	Pérdida	No existe control de préstamo		5	3	15
ESTABILIZADOR	RFZ157	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DIRECTOR	4	2	8
	RFZ158	Rayo	No existe un pararrayos que proteja ante descargas eléctricas		4	2	8
	RFZ159	Polvo	Falta de limpieza constante del equipo		2	2	4
	RFZ160	Fallas en los equipos	No existe reemplazo inmediato del equipo		4	2	8
	RFZ161	Corte de energía	No existe UPS		4	3	12
	RFZ162	Robo	Falta de controles físicos		4	4	16
FOTOCOPIADORA EN GENERAL	RFZ163	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DIRECTOR	4	2	8
	RFZ164	Rayo	No existe un pararrayos que proteja ante descargas eléctricas		4	2	8
	RFZ165	Polvo	Falta de limpieza constante del equipo		2	2	4

	RFZ166	Fallas en los equipos	No existe reemplazo inmediato del equipo		5	3	15
	RFZ167	Corte de energía	No existe UPS		5	2	10
	RFZ168	Error de configuración	No existe manual de usuario		3	3	9
	RFZ169	Error de usuario	Desconocimiento de uso		3	2	6
	RFZ170	Acceso sin autorización	Cualquier usuario puede utilizarlo sin permiso		3	2	6
IMPRESORAS	RFZ171	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DIRECTOR	4	2	8
	RFZ172	Rayo	No existe un pararrayos que proteja ante descargas eléctricas		4	2	8
	RFZ173	Polvo	Falta de limpieza constante del equipo		2	2	4
	RFZ174	Fallas en los equipos	No existe reemplazo inmediato del equipo		5	3	15
	RFZ175	Corte de energía	No existe UPS		5	2	10
	RFZ176	Error de configuración	Manual de usuario almacenado en otro lugar		3	3	9
	RFZ177	Error de usuario	Desconocimiento de uso		3	2	6
REPRODUCTOR DE VIDEO	RFZ178	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	DIRECTOR	4	1	4
	RFZ179	Fallas en los equipos	No existe reemplazo inmediato del equipo		4	3	12
	RFZ180	Corte de energía	No existe UPS		4	2	8
	RFZ181	Error de usuario	Manipulación inadecuada		4	2	8

SERVIDOR	RFZ182	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	CIST	4	1	4
	RFZ183	Rayo	No existe un pararrayos que proteja ante descargas eléctricas		4	1	4
	RFZ184	Polvo	Falta de limpieza constante del equipo		3	2	6
	RFZ185	Fallas en los equipos	No existe reemplazo inmediato del equipo		4	3	12
	RFZ186	Corte de energía	No existe UPS		4	2	8
	RFZ187	Error de usuario	Manipulación inadecuada		3	3	9
PROYECTOR MULTIMEDIA	RFZ188	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DOCENTE ASIGNADO	4	1	4
	RFZ189	Rayo	No existe un pararrayos que proteja ante descargas eléctricas		3	1	3
	RFZ190	Fallas en los equipos	No existe reemplazo inmediato del equipo		4	2	8
	RFZ191	Corte de energía	No existe UPS		4	2	8
	RFZ192	Error de usuario	Manipulación inadecuada		4	2	8
	RFZ193	Error de mantenimiento de Hardware	Manual de usuario no disponible		3	2	6
	RFZ194		Desconocimiento del usuario		3	1	3
	RFZ195		Mal uso del lente óptico		5	2	10
	RFZ196	Robo	Puertas de acceso siempre abiertas		5	4	20

TELEVISOR LED	RFZ197	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DOCENTE ASIGNADO	4	2	8
	RFZ198	Rayo	No existe un pararrayos que proteja ante descargas eléctricas		4	2	8
	RFZ199	Fallas en los equipos	No existe reemplazo inmediato del equipo		4	2	8
	RFZ200	Corte de energía	No existe UPS		3	2	6
	RFZ201	Error de usuario	Manipulación inadecuada		3	1	3
	RFZ202	Error de mantenimiento de Hardware	Uso de implementos de limpieza inadecuados		3	1	3
	RFZ203	Robo	Puertas de acceso siempre abiertas		5	4	20
UNIDAD CENTRAL DE PROCESO - CPU	RFZ204	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	SECRETARIA	4	1	4
	RFZ205	Rayo	No existe un pararrayos que proteja ante descargas eléctricas		4	1	4
	RFZ206	Polvo	Falta de limpieza constante del equipo		3	2	6
	RFZ207	Fallas en los equipos	No existe reemplazo inmediato del equipo		5	2	10
	RFZ208	Corte de energía	No existe UPS		4	3	12
	RFZ209	Error de administrador	Falta de software administrador de núcleo (protección de partituras del disco)		4	4	16
	RFZ210		Contraseña de inicio de sesión inexistente		4	4	16
	RFZ211	Error de configuración	Falta de software administrador de núcleo (protección de partituras del disco)		4	3	12

	RFZ212	Error de usuario	Falta de software administrador de núcleo (protección de partituras del disco)		3	3	9
	RFZ213	Aparición de virus o malware	Falta de programas antivirus/antimalware		4	3	12
	RFZ214		Descargas de software no seguras.		4	4	16
	RFZ215	Sobrecalentamiento	Batería malograda, funciona siempre conectado a la energía		4	2	8
	RFZ216	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)		4	2	8
	RFZ217	Error de actualización de Software	Descargas de software no seguras.		4	3	12
	RFZ218		Software obsoleto		4	3	12
	RFZ219	Error de mantenimiento de Software	Manual de usuario inexistente		4	1	4
	RFZ220		Desconocimiento del usuario		4	1	4
	RFZ221	Error de mantenimiento de Hardware	Desconocimiento del usuario		4	1	4
	RFZ222	Exceso de confianza	El personal confía sus claves a personal de confianza		4	5	20
	RFZ223	Manipulación de configuraciones	Falta de software administrador de núcleo (protección de partituras del disco)		3	3	9
	RFZ224		Contraseña de inicio de sesión inexistente		4	4	16
	RFZ225	Insertar virus o malware	Falta de programas antivirus/antimalware		4	3	12
	RFZ226	Acceso sin autorización	Contraseña de inicio de sesión inexistente		4	5	20
	RFZ227	Eliminación de información digital	Falta de copias de seguridad		4	4	16
	RFZ228		Contraseña de inicio de sesión inexistente		4	4	16
	RFZ229	Robo de equipos	Falta de medidas de seguridad física		5	3	15

CÁMARA DE VIGILANCIA	RFZ230	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	DIRECTOR	4	2	8
	RFZ231	Polvo	Falta de limpieza constante del equipo		2	2	4
	RFZ232	Fallas en los equipos	No existe reemplazo inmediato del equipo		4	2	8
	RFZ233	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)		5	2	10
	RFZ234	Error de actualización de Software	Software obsoleto		2	2	4
	RFZ235	Acceso sin autorización	Contraseña de inicio de sesión inexistente		4	3	12
	RFZ236	Eliminación de información digital	Falta de copias de seguridad		4	4	16
	RFZ237		Contraseña de inicio de sesión inexistente		4	4	16
	RFZ238	Robo de equipos	Falta de medidas de seguridad física		4	3	12
LIBRO DE INCIDENCIAS	RFZ239	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DIRECTOR	5	2	10
	RFZ240	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo		5	2	10
	RFZ241	Borrar información	Falta de copias de seguridad		5	2	10
	RFZ242	Robo o pérdida	Pocos o nulos controles de acceso		4	1	4
	RFZ243	Suplantación de identidad	Falta de políticas de autenticación		4	1	4

CUADERNO DE ATENCIONES	RFZ244	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	COORDINADOR DE TUTORÍA	3	2	6
	RFZ245	Borrar información	Falta de copias de seguridad		3	2	6
	RFZ246	Robo o pérdida	Pocos o nulos controles de acceso		3	1	3
	RFZ247	Suplantación de identidad	Falta de políticas de autenticación		3	2	6
CUADERNO DE INCIDENCIAS	RFZ248	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	PSICÓLOGO	3	2	6
	RFZ249	Borrar información	Falta de copias de seguridad		3	2	6
	RFZ250	Robo o pérdida	Pocos o nulos controles de acceso		3	1	3
	RFZ251	Suplantación de identidad	Falta de políticas de autenticación		3	2	6
ACTA DE EVALUACIÓN Y CERTIFICADO DE ESTUDIOS	RFZ252	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DIRECTOR	5	2	10
	RFZ253	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo		5	3	15
	RFZ254	Borrar información	Falta de copias de seguridad		5	2	10
	RFZ255	Robo o pérdida	Pocos o nulos controles de acceso		5	3	15

FICHAS DE MONITOREO CIENCIAS	RFZ256	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	COORDINADOR DE CIENCIAS	5	1	5
	RFZ257	Borrar información	Falta de copias de seguridad		5	2	10
	RFZ258	Robo o pérdida	Pocos o nulos controles de acceso		5	3	15
	RFZ259	Suplantación de identidad	Falta de políticas de autenticación		5	3	15
FICHAS DE MONITOREO LETRAS	RFZ260	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	COORDINADOR DE LETRAS	5	1	5
	RFZ261	Borrar información	Falta de copias de seguridad		5	2	10
	RFZ262	Robo o pérdida	Pocos o nulos controles de acceso		5	3	15
	RFZ263	Suplantación de identidad	Falta de políticas de autenticación		5	3	15
REG. DE ASISTENCIA TRABAJADORES	RFZ264	Borrar información	Falta de copias de seguridad	DIRECTOR	5	2	10
	RFZ265	Robo o pérdida	Pocos o nulos controles de acceso		5	2	10
REG. DE ASISTENCIA ESTUDIANTES	RFZ266	Borrar información	Falta de copias de seguridad	AUXILIAR	5	2	10
	RFZ267	Robo o pérdida	Pocos o nulos controles de acceso		5	1	5

MEMORÁNDUMS	RFZ268	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	DIRECTOR	5	3	15
	RFZ269	Borrar información	Falta de copias de seguridad		5	1	5
	RFZ270	Robo o pérdida	Pocos o nulos controles de acceso		5	2	10
	RFZ271	Suplantación de identidad	Falta de políticas de autenticación		5	1	5
BOLETA DE NOTAS	RFZ272	Borrar información	Falta de copias de seguridad	DIRECTOR	5	3	15
	RFZ273	Robo o pérdida	Pocos o nulos controles de acceso		5	2	10
CONTRASEÑAS DE EQUIPOS	RFZ274	Error de configuración	Configuración poco segura puede ser explotada	CIST	4	3	12
	RFZ275	Ingeniería social	Desconocimiento del personal a diferentes tipos de ataques		4	2	8
	RFZ276	Exceso de confianza	El personal confía sus claves a personal de confianza		4	4	16
REGLAMENTO INTERNO INSTITUCIONAL	RFZ277	Borrar información	Falta de copias de seguridad	DIRECTOR	4	3	12
	RFZ278	Robo o pérdida	Pocos o nulos controles de acceso		5	2	10
PLAN ANUAL DE TRABAJO	RFZ279	Borrar información	Falta de copias de seguridad	DIRECTOR	4	3	12
	RFZ280	Robo o pérdida	Pocos o nulos controles de acceso		5	2	10

PROYECTO EDUCATIVO INSTITUCIONAL	RFZ281	Borrar información	Falta de copias de seguridad	DIRECTOR	4	3	12
	RFZ282	Robo o pérdida	Pocos o nulos controles de acceso		5	2	10
SISTEMA OPERATIVO WIN10	RFZ283	Error de configuración	Configuración predeterminada no óptima para los equipos	CIST	4	3	12
	RFZ284	Error de administración	Débil gestión de contraseñas		4	3	12
	RFZ285	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)		5	4	20
	RFZ286	Aparición de virus o malware	Falta de programas antivirus/antimalware		4	3	12
	RFZ287		Descargas de software no seguras.		4	3	12
	RFZ288	Licencia ilegal de software	Ataques de tipo rasomware		5	2	10
SISTEMA OPERATIVO WIN8 PRO	RFZ289	Error de configuración	Configuración predeterminada no óptima para los equipos	CIST	4	3	12
	RFZ290	Error de administración	Débil gestión de contraseñas		4	3	12
	RFZ291	Error de actualización de Software	Software desfasado para la actualidad		5	5	25
	RFZ292	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)		4	4	16
	RFZ293	Aparición de virus o malware	Falta de programas antivirus/antimalware		4	3	12
	RFZ294		Descargas de software no seguras.		4	3	12
	RFZ295	Licencia ilegal de software	Ataques de tipo rasomware		5	4	20

MICROSOFT OFFICE 2013	RFZ296	Error de configuración	Configuración predeterminada no óptima para los equipos	CIST	3	3	9
	RFZ297	Error de actualización de Software	Software desfasado para la actualidad		3	4	12
	RFZ298	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)		4	3	12
	RFZ299	Licencia ilegal de software	Ataques de tipo rasomware		4	4	16
MICROSOFT OFFICE 2016	RFZ300	Error de configuración	Configuración predeterminada no óptima para los equipos	CIST	3	3	9
	RFZ301	Error de actualización de Software	Software desfasado para la actualidad		3	3	9
	RFZ302	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)		4	3	12
	RFZ303	Licencia ilegal de software	Ataques de tipo rasomware		4	3	12
SCRATCH V3	RFZ304	Error de configuración	Configuración predeterminada no óptima para los equipos	CIST	3	2	6
	RFZ305	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)		2	2	4
XMIND	RFZ306	Error de configuración	Configuración predeterminada no óptima para los equipos	CIST	2	2	4
	RFZ307	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)		2	2	4
CMAPTOOLS	RFZ308	Error de configuración	Configuración predeterminada no óptima para los equipos	CIST	2	2	4
	RFZ309	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)		2	2	4

MODEM ROUTER	RFZ310	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	DIRECTOR	4	2	8
	RFZ311	Rayo	No existe un pararrayos que proteja ante descargas eléctricas		4	1	4
	RFZ312	Polvo	Falta de limpieza constante del equipo		3	2	6
	RFZ313	Fallas en los equipos	No existe reemplazo inmediato del equipo		4	3	12
	RFZ314	Corte de energía	No existe UPS		4	2	8
	RFZ315	Error de usuario	Manipulación inadecuada		3	2	6
DOCENTES	RFZ316	Ingeniería social	Desconocimiento de tipos de ataques maliciosos	DOCENTE	4	4	16
	RFZ317	Suplantación de identidad	Exceso de confianza		4	3	12
	RFZ318	Acceso sin autorización	Descuido del personal de vigilancia		4	3	12
PERSONAL ADMINISTRATIVO	RFZ319	Ingeniería social	Desconocimiento de tipos de ataques maliciosos	PERSONAL ADMINISTRATIVO	5	4	20
	RFZ320	Suplantación de identidad	Exceso de confianza		5	5	25
	RFZ321	Acceso sin autorización	Descuido del personal de vigilancia		4	2	8
	RFZ322	Personal no disponible	Falta de presupuesto para contratar personal calificado para el puesto		5	2	10
ESTUDIANTES	RFZ323	Mal uso de los recursos	Desconocimiento del uso de las laptops	DOCENTE ASIGNADO	4	2	8
	RFZ324	Mal uso del hardware	Maltrato a los equipos		4	1	4

Nota: Descripción de los activos sus vulnerabilidades, riesgos.

Tratamiento del riesgo

TABLA XIII. TRATAMIENTO DEL RIESGO.

ACTIVO	ID DE RIESGO	AMENAZA	VULNERABILIDAD	TRATAMIENTO	JUSTIFICACIÓN
AMPLIFICADOR DE AUDIO	RFZ01	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ02	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	Reducir el riesgo	Implementar un pararrayos básico en un lugar estratégico a fin de evitar descargas eléctricas a los equipos
	RFZ03	Polvo	Falta de limpieza constante del equipo	Evitar el riesgo	Crear una política de limpieza de los equipos
	RFZ04	Fallas en los equipos	No existe reemplazo inmediato del equipo	Transferir el riesgo	Tener un equipo listo para reemplazo
	RFZ05	Corte de energía	No existe UPS	Evitar el riesgo	Comprar un UPS
	RFZ06	Error de configuración	No existe manual de uso	Asumir el riesgo	Capacitar a los usuarios a fin de orientar en el buen uso de los equipos
	RFZ07	Error de mantenimiento de hardware	No existe manual de uso	Evitar el riesgo	Obtener el manual de uso guardado en el almacén
	RFZ08	Pérdida del equipo	El equipo es prestado a cualquier usuario que lo necesite	Reducir el riesgo	Crear un control de préstamo
	RFZ09		Falta de medidas de seguridad física	Reducir el riesgo	Crear una política de seguridad física
	RFZ10	Insertar virus o malware	Falta de programas antivirus	Reducir el riesgo	Crear protección contra código malicioso
	RFZ11		Descarga de software no seguras	Reducir el riesgo	Crear protección contra código malicioso
	RFZ12	Robo del equipo	Lugar de almacenamiento poco seguro	Reducir el riesgo	Crear una política de seguridad física

ARCHIVADOR DE MADERA	RFZ13	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ14	Polvo	Falta de limpieza constante del equipo	Evitar el riesgo	Crear una política de limpieza de los equipos
	RFZ15	Pérdida	Falta de medidas de seguridad física	Reducir el riesgo	Crear una política de seguridad física
	RFZ16	Robo	Lugar de almacenamiento poco seguro	Reducir el riesgo	Crear una política de seguridad física
ARCHIVADOR DE METAL	RFZ17	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ18	Polvo	Falta de limpieza constante del equipo	Evitar el riesgo	Crear una política de limpieza de los equipos
	RFZ19	Pérdida	Falta de medidas de seguridad física	Reducir el riesgo	Crear una política de seguridad física
	RFZ20	Robo	Lugar de almacenamiento poco seguro	Reducir el riesgo	Crear una política de seguridad física
ARMARIO DE METAL	RFZ21	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ22	Polvo	Falta de limpieza constante del equipo	Evitar el riesgo	Crear una política de limpieza de los equipos
	RFZ23	Pérdida	Falta de medidas de seguridad física	Reducir el riesgo	Crear una política de seguridad física
	RFZ24	Robo	Puerta de acceso siempre abierta	Reducir el riesgo	Crear una política de seguridad física

ARMARIO DE METAL	RFZ25	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ26	Polvo	Falta de limpieza constante del equipo	Evitar el riesgo	Crear una política de limpieza de los equipos
	RFZ27	Pérdida	Falta de medidas de seguridad física	Reducir el riesgo	Crear una política de seguridad física
	RFZ28	Robo	Puerta de acceso con cerradura sin funcionar	Reducir el riesgo	Crear una política de seguridad física
COMPUTADORA PERSONAL PORTÁTIL DE DIRECCIÓN	RFZ29	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ30	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	Reducir el riesgo	Implementar un pararrayos básico en un lugar estratégico a fin de evitar descargas eléctricas a los equipos
	RFZ31	Polvo	Falta de limpieza constante del equipo	Evitar el riesgo	Crear una política de limpieza de los equipos
	RFZ32	Fallas en los equipos	No existe reemplazo inmediato del equipo	Transferir el riesgo	Tener un equipo listo para reemplazo
	RFZ33	Corte de energía	No existe UPS	Evitar el riesgo	Comprar un UPS
	RFZ34		Batería malograda, funciona siempre conectado a la energía	Evitar el riesgo	Comprar un reemplazo de batería
	RFZ35	Error de administrador	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
	RFZ36		Contraseña de inicio de sesión inexistente	Reducir el riesgo	Crear política de contraseñas seguras
	RFZ37	Error de configuración	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
	RFZ38	Error de usuario	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze) Crear un programa de capacitación

	RFZ39	Aparición de virus o malware	Falta de programas antivirus/antimalware	Reducir el riesgo	Instalar un programa antivirus y antimalware
	RFZ40		Descargas de software no seguras.	Reducir el riesgo	Crear protección contra código malicioso Crear un programa de capacitación
	RFZ41	Sobrecalentamiento	Batería malograda, funciona siempre conectado a la energía	Evitar el riesgo	Comprar un reemplazo de batería
	RFZ42	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	Reducir el riesgo	Instalar un programa administrador de núcleo (DeepFreeze) Crear una política de control de accesos
	RFZ43	Error de actualización de Software	Descargas de software no seguras.	Reducir el riesgo	Crear protección contra código malicioso Crear un programa de capacitación
	RFZ44		Software obsoleto	Reducir el riesgo	Actualizar la versión del software
	RFZ45	Error de mantenimiento de Software	Manual de usuario no disponible	Evitar el riesgo	Tener disponible el manual de uso guardado en el almacén
	RFZ46		Desconocimiento del usuario	Reducir el riesgo	Crear un programa de capacitación
	RFZ47	Error de mantenimiento de Hardware	Manual de usuario no disponible	Evitar el riesgo	Tener disponible el manual de uso guardado en el almacén
	RFZ48		Desconocimiento del usuario	Reducir el riesgo	Crear un programa de capacitación
	RFZ49	Manipulación de configuraciones	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
	RFZ50		Contraseña de inicio de sesión inexistente	Reducir el riesgo	Crear política de contraseñas seguras
	RFZ51	Insertar virus o malware	Falta de programas antivirus/antimalware	Reducir el riesgo	Instalar un programa antivirus y antimalware
	RFZ52	Acceso sin autorización	Contraseña de inicio de sesión inexistente	Reducir el riesgo	Crear política de control de acceso
	RFZ53	Eliminación de información digital	Falta de copias de seguridad	Reducir el riesgo	Crear política de seguridad de operaciones, copias de respaldo
	RFZ54		Contraseña de inicio de sesión inexistente	Reducir el riesgo	Crear política de control de acceso
	RFZ55	Robo de equipos	Falta de medidas de seguridad física	Reducir el riesgo	Crear política de seguridad física

COMPUTADORA PERSONAL PORTÁTIL DE DOCENTE	RFZ56	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ57	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	Reducir el riesgo	Implementar un pararrayos básico en un lugar estratégico a fin de evitar descargas eléctricas a los equipos
	RFZ58	Polvo	Falta de limpieza constante del equipo	Evitar el riesgo	Crear una política de limpieza de los equipos
	RFZ59	Fallas en los equipos	No existe reemplazo inmediato del equipo	Transferir el riesgo	Tener un equipo listo para reemplazo
	RFZ60	Corte de energía	No existe UPS	Evitar el riesgo	Comprar un UPS
	RFZ61		Batería malograda, funciona siempre conectado a la energía	Evitar el riesgo	Comprar un reemplazo de batería
	RFZ62	Error de administrador	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
	RFZ63		Contraseña de inicio de sesión inexistente	Reducir el riesgo	Crear política de contraseñas seguras
	RFZ64	Error de configuración	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
	RFZ65	Error de usuario	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze) Crear un programa de capacitación
	RFZ66	Aparición de virus o malware	Falta de programas antivirus/antimalware	Reducir el riesgo	Instalar un programa antivirus y antimalware
	RFZ67		Descargas de software no seguras.	Reducir el riesgo	Crear protección contra código malicioso Crear un programa de capacitación
	RFZ68	Sobrecalentamiento	Batería malograda, funciona siempre conectado a la energía	Evitar el riesgo	Comprar un reemplazo de batería

	RFZ69	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	Reducir el riesgo	Instalar un programa administrador de núcleo (DeepFreeze) Crear una política de control de accesos
	RFZ70	Error de actualización de Software	Descargas de software no seguras.	Reducir el riesgo	Crear protección contra código malicioso Crear un programa de capacitación
	RFZ71		Software obsoleto	Reducir el riesgo	Actualizar la versión del software
	RFZ72	Error de mantenimiento de Software	Manual de usuario no disponible	Evitar el riesgo	Tener disponible el manual de uso guardado en el almacén
	RFZ73		Desconocimiento del usuario	Reducir el riesgo	Crear un programa de capacitación
	RFZ74	Error de mantenimiento de Hardware	Manual de usuario no disponible	Evitar el riesgo	Tener disponible el manual de uso guardado en el almacén
	RFZ75		Desconocimiento del usuario	Reducir el riesgo	Crear un programa de capacitación
	RFZ76	Manipulación de configuraciones	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
	RFZ77		Contraseña de inicio de sesión inexistente	Reducir el riesgo	Crear política de contraseñas seguras
	RFZ78	Insertar virus o malware	Falta de programas antivirus/antimalware	Reducir el riesgo	Instalar un programa antivirus y antimalware
	RFZ79	Acceso sin autorización	Contraseña de inicio de sesión inexistente	Reducir el riesgo	Crear política de control de acceso
	RFZ80	Eliminación de información digital	Falta de copias de seguridad	Reducir el riesgo	Crear política de seguridad de operaciones, copias de respaldo
	RFZ81		Contraseña de inicio de sesión inexistente	Reducir el riesgo	Crear política de control de acceso
	RFZ82	Robo de equipos	Falta de medidas de seguridad física	Reducir el riesgo	Crear política de seguridad física

COMPUTADORA PERSONAL PORTÁTIL DE ESTUDIANTE	RFZ83	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ84	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	Reducir el riesgo	Implementar un pararrayos básico en un lugar estratégico a fin de evitar descargas eléctricas a los equipos
	RFZ85	Polvo	Falta de limpieza constante del equipo	Evitar el riesgo	Crear una política de limpieza de los equipos
	RFZ86	Fallas en los equipos	No existe reemplazo inmediato del equipo	Transferir el riesgo	Tener un equipo listo para reemplazo
	RFZ87	Corte de energía	No existe UPS	Evitar el riesgo	Comprar un UPS
	RFZ88		Batería malograda, funciona siempre conectado a la energía	Evitar el riesgo	Comprar un reemplazo de batería
	RFZ89	Error de administrador	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
	RFZ90		Contraseña de inicio de sesión visible en la web	Reducir el riesgo	Crear política de contraseñas seguras
	RFZ91	Error de configuración	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
	RFZ92	Error de usuario	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze) Crear un programa de capacitación
	RFZ93	Aparición de virus o malware	Falta de programas antivirus/antimalware	Reducir el riesgo	Instalar un programa antivirus y antimalware
	RFZ94		Descargas de software no seguras.	Reducir el riesgo	Crear protección contra código malicioso Crear un programa de capacitación
	RFZ95	Sobrecalentamiento	Batería malograda, funciona siempre conectado a la energía	Evitar el riesgo	Comprar un reemplazo de batería

	RFZ96	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	Reducir el riesgo	Instalar un programa administrador de núcleo (DeepFreeze) Crear una política de control de accesos
	RFZ97	Error de actualización de Software	Descargas de software no seguras.	Reducir el riesgo	Crear protección contra código malicioso Crear un programa de capacitación
	RFZ98		Software obsoleto	Reducir el riesgo	Actualizar la versión del software
	RFZ99	Error de mantenimiento de Software	Manual de usuario no disponible	Evitar el riesgo	Tener disponible el manual de uso guardado en el almacén
	RFZ100		Desconocimiento del usuario	Reducir el riesgo	Crear un programa de capacitación
	RFZ101	Error de mantenimiento de Hardware	Manual de usuario no disponible	Evitar el riesgo	Tener disponible el manual de uso guardado en el almacén
	RFZ102		Desconocimiento del usuario	Reducir el riesgo	Crear un programa de capacitación
	RFZ103	Manipulación de configuraciones	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo(DeepFreeze)
	RFZ104		Contraseña de inicio de sesión visibles en la web	Reducir el riesgo	Crear política de contraseñas seguras
	RFZ105	Insertar virus o malware	Falta de programas antivirus/antimalware	Reducir el riesgo	Instalar un programa antivirus y antimalware
	RFZ106	Acceso sin autorización	Contraseña de inicio de sesión visible en la web	Reducir el riesgo	Crear política de control de acceso
	RFZ107	Eliminación de información digital	Falta de copias de seguridad	Reducir el riesgo	Crear política de seguridad de operaciones, copias de respaldo
	RFZ108		Contraseña de inicio de sesión débil	Reducir el riesgo	Crear política de control de acceso
	RFZ109	Robo de equipos	Falta de medidas de seguridad física	Reducir el riesgo	Crear política de seguridad física

COMPUTADORA PERSONAL PORTÁTIL ALMACENADA	RFZ110	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ111	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	Reducir el riesgo	Implementar un pararrayos básico en un lugar estratégico a fin de evitar descargas eléctricas a los equipos
	RFZ112	Polvo	Falta de limpieza constante del equipo	Evitar el riesgo	Crear una política de limpieza de los equipos
	RFZ113	Fallas en los equipos	No existe reemplazo inmediato del equipo	Transferir el riesgo	Tener un equipo listo para reemplazo
	RFZ114	Corte de energía	No existe UPS	Evitar el riesgo	Comprar un UPS
	RFZ115		Batería malograda, funciona siempre conectado a la energía	Evitar el riesgo	Comprar un reemplazo de batería
	RFZ116	Error de administrador	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo(DeepFreeze)
	RFZ117		Contraseña de inicio de sesión inexistente	Reducir el riesgo	Crear política de contraseñas seguras
	RFZ118	Error de configuración	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
	RFZ119	Error de usuario	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze) Crear un programa de capacitación
	RFZ120	Aparición de virus o malware	Falta de programas antivirus/antimalware	Reducir el riesgo	Instalar un programa antivirus y antimalware
	RFZ121		Descargas de software no seguras.	Reducir el riesgo	Crear protección contra código malicioso Crear un programa de capacitación
	RFZ122	Sobrecalentamiento	Batería malograda, funciona siempre conectado a la energía	Evitar el riesgo	Comprar un reemplazo de batería

	RFZ123	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	Reducir el riesgo	Instalar un programa administrador de núcleo (DeepFreeze) Crear una política de control de accesos
	RFZ124	Error de actualización de Software	Descargas de software no seguras.	Reducir el riesgo	Crear protección contra código malicioso Crear un programa de capacitación
	RFZ125		Software obsoleto	Reducir el riesgo	Actualizar la versión del software
	RFZ126	Error de mantenimiento de Software	Manual de usuario no disponible	Evitar el riesgo	Tener disponible el manual de uso guardado en el almacén
	RFZ127		Desconocimiento del usuario	Reducir el riesgo	Crear un programa de capacitación
	RFZ128	Error de mantenimiento de Hardware	Manual de usuario no disponible	Evitar el riesgo	Tener disponible el manual de uso guardado en el almacén
	RFZ129		Desconocimiento del usuario	Reducir el riesgo	Crear un programa de capacitación
	RFZ130	Manipulación de configuraciones	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
	RFZ131		Contraseña de inicio de sesión inexistente	Reducir el riesgo	Crear política de contraseñas seguras
	RFZ132	Insertar virus o malware	Falta de programas antivirus/antimalware	Reducir el riesgo	Instalar un programa antivirus y antimalware
	RFZ133	Acceso sin autorización	Contraseña de inicio de sesión inexistente	Reducir el riesgo	Crear política de control de acceso
	RFZ134	Eliminación de información digital	Falta de copias de seguridad	Reducir el riesgo	Crear política de seguridad de operaciones, copias de respaldo
	RFZ135		Contraseña de inicio de sesión inexistente	Reducir el riesgo	Crear política de control de acceso
	RFZ136	Robo de equipos	Falta de medidas de seguridad física	Reducir el riesgo	Crear política de seguridad física

CONSOLA PARA CONTROL DE AUDIO	RFZ137	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ138	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	Reducir el riesgo	Implementar un pararrayos básico en un lugar estratégico a fin de evitar descargas eléctricas a los equipos
	RFZ139	Polvo	Falta de limpieza constante del equipo	Evitar el riesgo	Crear una política de limpieza de los equipos
	RFZ140	Fallas en los equipos	No existe reemplazo inmediato del equipo	Asumir el riesgo	Existe otros equipos que pueden realizar una función similar
	RFZ141	Corte de energía	No existe UPS	Reducir el riesgo	Comprar un UPS
DISCO DURO EXTERNO	RFZ142	Error de configuración	No existe manual de usuario	Reducir el riesgo	Comprar extintor de incendios
	RFZ143	Error de usuario	Descarga de programas de dudosa procedencia	Reducir el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
	RFZ144	Aparición de virus o malware	Falta de programas antivirus/antimalware	Reducir el riesgo	Instalar un programa antivirus y antimalware
	RFZ145		Descargas de software no seguras.	Reducir el riesgo	Crear protección contra código malicioso Crear un programa de capacitación
	RFZ146	Sobrecalentamiento	Uso excesivo del equipo	Reducir el riesgo	Crear una política de seguridad de operaciones
	RFZ147	Borrar información	No existe copias de respaldo	Reducir el riesgo	Crear política de seguridad de operaciones, copias de respaldo
	RFZ148	Pérdida	No existe control de préstamo	Reducir el riesgo	Crear un control de préstamo
	RFZ149	Robo	No existe lugar seguro de almacenamiento	Reducir el riesgo	Crear política de seguridad física

EQUIPO DE SONIDO	RFZ150	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ151	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	Reducir el riesgo	Implementar un pararrayos básico en un lugar estratégico a fin de evitar descargas eléctricas a los equipos
	RFZ152	Polvo	Falta de limpieza constante del equipo	Evitar el riesgo	Crear una política de limpieza de los equipos
	RFZ153	Fallas en los equipos	No existe reemplazo inmediato del equipo	Asumir el riesgo	Existe otros equipos que pueden realizar una función similar
	RFZ154	Corte de energía	No existe UPS	Reducir el riesgo	Comprar un UPS
	RFZ155	Robo	Cerradura de puerta no sirve	Reducir el riesgo	Comprar una cerradura confiable
	RFZ156	Pérdida	No existe control de préstamo	Reducir el riesgo	Crear un control de préstamo
ESTABILIZADOR	RFZ157	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ158	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	Reducir el riesgo	Implementar un pararrayos básico en un lugar estratégico a fin de evitar descargas eléctricas a los equipos
	RFZ159	Polvo	Falta de limpieza constante del equipo	Evitar el riesgo	Crear una política de limpieza de los equipos
	RFZ160	Fallas en los equipos	No existe reemplazo inmediato del equipo	Asumir el riesgo	Existe otros equipos que pueden realizar una función similar
	RFZ161	Corte de energía	No existe UPS	Reducir el riesgo	Comprar un UPS
	RFZ162	Robo	Falta de controles físicos	Reducir el riesgo	Crear una política de seguridad física

FOTOCOPIADORA EN GENERAL	RFZ163	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ164	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	Reducir el riesgo	Implementar un pararrayos básico en un lugar estratégico a fin de evitar descargas eléctricas a los equipos
	RFZ165	Polvo	Falta de limpieza constante del equipo	Evitar el riesgo	Crear una política de limpieza de los equipos
	RFZ166	Fallas en los equipos	No existe reemplazo inmediato del equipo	Asumir el riesgo	Existe otros equipos que pueden realizar una función similar
	RFZ167	Corte de energía	No existe UPS	Reducir el riesgo	Comprar un UPS
	RFZ168	Error de configuración	No existe manual de usuario	Evitar el riesgo	Tener el manual de usuario disponible el cual está guardado en almacén
	RFZ169	Error de usuario	Desconocimiento de uso	Reducir el riesgo	Crear un plan de capacitación
	RFZ170	Acceso sin autorización	Cualquier usuario puede utilizarlo sin permiso	Reducir el riesgo	Crear una política de control de accesos
IMPRESORAS	RFZ171	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ172	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	Reducir el riesgo	Implementar un pararrayos básico en un lugar estratégico a fin de evitar descargas eléctricas a los equipos
	RFZ173	Polvo	Falta de limpieza constante del equipo	Evitar el riesgo	Crear una política de limpieza de los equipos
	RFZ174	Fallas en los equipos	No existe reemplazo inmediato del equipo	Reducir el riesgo	Realizar el mantenimiento preventivo del equipo
	RFZ175	Corte de energía	No existe UPS	Reducir el riesgo	Comprar un UPS
	RFZ176	Error de configuración	Manual de usuario almacenado en otro lugar	Evitar el riesgo	Tener el manual de usuario disponible el cual está guardado en almacén
	RFZ177	Error de usuario	Desconocimiento de uso	Reducir el riesgo	Crear un plan de capacitación

REPRODUCTOR DE VIDEO	RFZ178	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	Reducir el riesgo	Implementar un pararrayos básico en un lugar estratégico a fin de evitar descargas eléctricas a los equipos
	RFZ179	Fallas en los equipos	No existe reemplazo inmediato del equipo	Reducir el riesgo	Realizar el mantenimiento preventivo del equipo
	RFZ180	Corte de energía	No existe UPS	Reducir el riesgo	Comprar un UPS
	RFZ181	Error de usuario	Manipulación inadecuada	Reducir el riesgo	Crear un plan de capacitación Crear una política de seguridad de operaciones
SERVIDOR	RFZ182	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ183	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	Reducir el riesgo	Implementar un pararrayos básico en un lugar estratégico a fin de evitar descargas eléctricas a los equipos
	RFZ184	Polvo	Falta de limpieza constante del equipo	Reducir el riesgo	Crear una política de limpieza de los equipos
	RFZ185	Fallas en los equipos	No existe reemplazo inmediato del equipo	Reducir el riesgo	Realizar el mantenimiento preventivo del equipo
	RFZ186	Corte de energía	No existe UPS	Reducir el riesgo	Comprar un UPS
	RFZ187	Error de usuario	Manipulación inadecuada	Reducir el riesgo	Crear un plan de capacitación Crear una política de seguridad de operaciones

PROYECTOR MULTIMEDIA	RFZ188	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ189	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	Reducir el riesgo	Implementar un pararrayos básico en un lugar estratégico a fin de evitar descargas eléctricas a los equipos
	RFZ190	Fallas en los equipos	No existe reemplazo inmediato del equipo	Reducir el riesgo	Realizar el mantenimiento preventivo del equipo
	RFZ191	Corte de energía	No existe UPS	Reducir el riesgo	Comprar un UPS
	RFZ192	Error de usuario	Manipulación inadecuada	Reducir el riesgo	Crear un plan de capacitación Crear una política de seguridad de operaciones
	RFZ193	Error de mantenimiento de Hardware	Manual de usuario no disponible	Evitar el riesgo	Tener el manual de usuario disponible el cual está guardado en almacén
	RFZ194		Desconocimiento del usuario	Reducir el riesgo	Crear un plan de capacitación Crear una política de seguridad de operaciones
	RFZ195		Mal uso del lente óptico	Reducir el riesgo	Crear un plan de capacitación Crear una política de seguridad de operaciones
	RFZ196	Robo	Puertas de acceso siempre abiertas	Reducir el riesgo	Crear política de control físico

TELEVISOR LED	RFZ197	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ198	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	Reducir el riesgo	Implementar un pararrayos básico en un lugar estratégico a fin de evitar descargas eléctricas a los equipos
	RFZ199	Fallas en los equipos	No existe reemplazo inmediato del equipo	Reducir el riesgo	Realizar el mantenimiento preventivo del equipo
	RFZ200	Corte de energía	No existe UPS	Reducir el riesgo	Comprar un UPS
	RFZ201	Error de usuario	Manipulación inadecuada	Reducir el riesgo	Crear un plan de capacitación Crear una política de seguridad de operaciones
	RFZ202	Error de mantenimiento de Hardware	Uso de implementos de limpieza inadecuados	Reducir el riesgo	Realizar el mantenimiento preventivo del equipo
	RFZ203	Robo	Puertas de acceso siempre abiertas	Reducir el riesgo	Crear política de control físico. Mantener las puertas cerradas

UNIDAD CENTRAL DE PROCESO - CPU	RFZ204	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ205	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	Reducir el riesgo	Implementar un pararrayos básico en un lugar estratégico a fin de evitar descargas eléctricas a los equipos
	RFZ206	Polvo	Falta de limpieza constante del equipo	Evitar el riesgo	Crear una política de limpieza de los equipos
	RFZ207	Fallas en los equipos	No existe reemplazo inmediato del equipo	Transferir el riesgo	Tener un equipo listo para reemplazo
	RFZ208	Corte de energía	No existe UPS	Evitar el riesgo	Comprar un UPS
	RFZ209	Error de administrador	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
	RFZ210		Contraseña de inicio de sesión inexistente	Reducir el riesgo	Crear política de control de acceso, crear una contraseña segura
	RFZ211	Error de configuración	Falta de software administrador de núcleo (protección de partituras del disco)	Reducir el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
	RFZ212	Error de usuario	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
	RFZ213	Aparición de virus o malware	Falta de programas antivirus/antimalware	Evitar el riesgo	Instalar un programa antivirus y antimalware
	RFZ214		Descargas de software no seguras.	Reducir el riesgo	Concientizar a los usuarios de las descargas de software de lugares no seguros
	RFZ215	Sobrecalentamiento	Batería malograda, funciona siempre conectado a la energía	Evitar el riesgo	Comprar un reemplazo de batería

	RFZ216	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze) Crear copias de seguridad
	RFZ217	Error de actualización de Software	Descargas de software no seguras.	Reducir el riesgo	Concientizar a los usuarios de las descargas de software de lugares no seguros
	RFZ218		Software obsoleto	Reducir el riesgo	Actualizar la versión del software
	RFZ219	Error de mantenimiento de Software	Manual de usuario inexistente	Reducir el riesgo	Actualizar la versión del software
	RFZ220		Desconocimiento del usuario	Evitar el riesgo	Tener disponible el manual de uso guardado en el almacén
	RFZ221	Error de mantenimiento de Hardware	Desconocimiento del usuario	Reducir el riesgo	Crear un programa de capacitación
	RFZ222	Exceso de confianza	El personal confía sus claves a personal de confianza	Evitar el riesgo	Tener disponible el manual de uso guardado en el almacén
	RFZ223	Manipulación de configuraciones	Falta de software administrador de núcleo (protección de partituras del disco)	Reducir el riesgo	Crear un programa de capacitación
	RFZ224		Contraseña de inicio de sesión inexistente	Evitar el riesgo	Crear política de contraseñas seguras, crear política de control de accesos
	RFZ225	Insertar virus o malware	Falta de programas antivirus/antimalware	Reducir el riesgo	Instalar un programa antivirus y antimalware
	RFZ226	Acceso sin autorización	Contraseña de inicio de sesión inexistente	Reducir el riesgo	Crear política de contraseñas seguras, crear política de control de accesos
	RFZ227	Eliminación de información digital	Falta de copias de seguridad	Reducir el riesgo	Crear política de seguridad de operaciones, copias de respaldo
	RFZ228		Contraseña de inicio de sesión inexistente	Reducir el riesgo	Crear política de contraseñas seguras
	RFZ229	Robo de equipos	Falta de medidas de seguridad física	Reducir el riesgo	Crear política de seguridad física

CÁMARA DE VIGILANCIA	RFZ230	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	Reducir el riesgo	Implementar un pararrayos básico en un lugar estratégico a fin de evitar descargas eléctricas a los equipos
	RFZ231	Polvo	Falta de limpieza constante del equipo	Evitar el riesgo	Crear una política de limpieza de los equipos
	RFZ232	Fallas en los equipos	No existe reemplazo inmediato del equipo	Transferir el riesgo	Tener un equipo listo para reemplazo, mantener guardada la información de los videos en la nube
	RFZ233	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze) Crear copias de seguridad
	RFZ234	Error de actualización de Software	Software obsoleto	Reducir el riesgo	Actualizar la versión del software
	RFZ235	Acceso sin autorización	Contraseña de inicio de sesión inexistente	Reducir el riesgo	Crear política de contraseñas seguras, crear política de control de accesos
	RFZ236	Eliminación de información digital	Falta de copias de seguridad	Reducir el riesgo	Crear copias de seguridad
	RFZ237		Contraseña de inicio de sesión inexistente	Reducir el riesgo	Crear política de contraseñas seguras, crear política de control de accesos
	RFZ238	Robo de equipos	Falta de medidas de seguridad física	Reducir el riesgo	Crear política de seguridad física

LIBRO DE INCIDENCIAS	RFZ239	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ240	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	Transferir el riesgo	Crear copias digitales del respectivo documento a un almacenamiento en la nube
	RFZ241	Borrar información	Falta de copias de seguridad	Reducir el riesgo	Crear copias digitales del respectivo documento
	RFZ242	Robo o pérdida	Pocos o nulos controles de acceso	Reducir el riesgo	Crear política de control de acceso
	RFZ243	Suplantación de identidad	Falta de políticas de autenticación	Reducir el riesgo	Crear política de control de acceso
CUADERNO DE ATENCIONES	RFZ244	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	Transferir el riesgo	Crear copias digitales del respectivo documento a un almacenamiento en la nube
	RFZ245	Borrar información	Falta de copias de seguridad	Reducir el riesgo	Crear copias digitales del respectivo documento
	RFZ246	Robo o pérdida	Pocos o nulos controles de acceso	Reducir el riesgo	Crear política de control de acceso
	RFZ247	Suplantación de identidad	Falta de políticas de autenticación	Reducir el riesgo	Crear política de control de acceso

CUADERNO DE INCIDENCIAS	RFZ248	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	Transferir el riesgo	Crear copias digitales del respectivo documento a un almacenamiento en la nube
	RFZ249	Borrar información	Falta de copias de seguridad	Reducir el riesgo	Crear copias digitales del respectivo documento
	RFZ250	Robo o pérdida	Pocos o nulos controles de acceso	Reducir el riesgo	Crear política de control de acceso
	RFZ251	Suplantación de identidad	Falta de políticas de autenticación	Reducir el riesgo	Crear política de control de acceso
ACTA DE EVALUACIÓN Y CERTIFICADO DE ESTUDIOS	RFZ252	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ253	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	Transferir el riesgo	Crear copias digitales del respectivo documento a un almacenamiento en la nube
	RFZ254	Borrar información	Falta de copias de seguridad	Reducir el riesgo	Crear copias digitales del respectivo documento
	RFZ255	Robo o pérdida	Pocos o nulos controles de acceso	Reducir el riesgo	Crear política de control de acceso
FICHAS DE MONITOREO CIENCIAS	RFZ256	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	Transferir el riesgo	Crear copias digitales del respectivo documento
	RFZ257	Borrar información	Falta de copias de seguridad	Reducir el riesgo	Crear copias digitales del respectivo documento
	RFZ258	Robo o pérdida	Pocos o nulos controles de acceso	Reducir el riesgo	Crear política de control de acceso
	RFZ259	Suplantación de identidad	Falta de políticas de autenticación	Reducir el riesgo	Crear política de control de acceso

FICHAS DE MONITOREO LETRAS	RFZ260	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	Transferir el riesgo	Crear copias digitales del respectivo documento a un almacenamiento en la nube
	RFZ261	Borrar información	Falta de copias de seguridad	Reducir el riesgo	Crear copias digitales del respectivo documento
	RFZ262	Robo o pérdida	Pocos o nulos controles de acceso	Reducir el riesgo	Crear política de control de acceso
	RFZ263	Suplantación de identidad	Falta de políticas de autenticación	Reducir el riesgo	Crear política de control de acceso
REG. DE ASISTENCIA TRABAJADORES	RFZ264	Borrar información	Falta de copias de seguridad	Reducir el riesgo	Crear política de control de acceso, crear una copia digital del documento
	RFZ265	Robo o pérdida	Pocos o nulos controles de acceso	Reducir el riesgo	Crear política de control de acceso
REG. DE ASISTENCIA ESTUDIANTES	RFZ266	Borrar información	Falta de copias de seguridad	Reducir el riesgo	Crear política de control de acceso, crear una copia digital del documento
	RFZ267	Robo o pérdida	Pocos o nulos controles de acceso	Reducir el riesgo	Crear política de control de acceso

MEMORÁNDUMS	RFZ268	Degradación en almacenamiento	Hojas débiles que se desgastan con el tiempo	Transferir el riesgo	Crear copias digitales del respectivo documento a un almacenamiento en la nube
	RFZ269	Borrar información	Falta de copias de seguridad	Reducir el riesgo	Crear copias digitales del respectivo documento
	RFZ270	Robo o pérdida	Pocos o nulos controles de acceso	Reducir el riesgo	Crear política de control de acceso
	RFZ271	Suplantación de identidad	Falta de políticas de autenticación	Reducir el riesgo	Crear política de control de acceso
BOLETA DE NOTAS	RFZ272	Borrar información	Falta de copias de seguridad	Reducir el riesgo	Crear política de control de acceso, crear una copia digital del documento
	RFZ273	Robo o pérdida	Pocos o nulos controles de acceso	Reducir el riesgo	Crear política de control de acceso
CONTRASEÑAS DE EQUIPOS	RFZ274	Error de configuración	Configuración poco segura puede ser explotada	Reducir el riesgo	Crear política de contraseñas seguras
	RFZ275	Ingeniería social	Desconocimiento del personal a diferentes tipos de ataques	Reducir el riesgo	Crear un plan de capacitación y concientización a usuarios
	RFZ276	Exceso de confianza	El personal confía sus claves a personal de confianza	Reducir el riesgo	Usar un sistema de gestión de contraseñas

REGLAMENTO INTERNO INSTITUCIONAL	RFZ277	Borrar información	Falta de copias de seguridad	Reducir el riesgo	Crear política de control de acceso, crear una copia digital del documento
	RFZ278	Robo o pérdida	Pocos o nulos controles de acceso	Reducir el riesgo	Crear política de control de acceso
PLAN ANUAL DE TRABAJO	RFZ279	Borrar información	Falta de copias de seguridad	Reducir el riesgo	Crear política de control de acceso, crear una copia digital del documento
	RFZ280	Robo o pérdida	Pocos o nulos controles de acceso	Reducir el riesgo	Crear política de control de acceso
PROYECTO EDUCATIVO INSTITUCIONAL	RFZ281	Borrar información	Falta de copias de seguridad	Reducir el riesgo	Crear política de control de acceso, crear una copia digital del documento
	RFZ282	Robo o pérdida	Pocos o nulos controles de acceso	Reducir el riesgo	Crear política de control de acceso
SISTEMA OPERATIVO WIN10	RFZ283	Error de configuración	Configuración predeterminada no óptima para los equipos	Reducir el riesgo	Crear un plan de acción para crear configuraciones óptimas que hagan más eficientes los recursos
	RFZ284	Error de administración	Débil gestión de contraseñas	Evitar el riesgo	Usar un sistema de gestión de contraseñas
	RFZ285	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
	RFZ286	Aparición de virus o malware	Falta de programas antivirus/antimalware	Reducir el riesgo	Instalar un programa antivirus y antimalware
	RFZ287		Descargas de software no seguras.	Reducir el riesgo	Crear un plan de capacitación y concientización a usuarios
	RFZ288	Licencia ilegal de software	Ataques de tipo ransomware	Reducir el riesgo	Instalar un programa antivirus y antimalware, instalar una licencia original

SISTEMA OPERATIVO WIN8 PRO	RFZ289	Error de configuración	Configuración predeterminada no óptima para los equipos	Reducir el riesgo	Crear un plan de acción para crear configuraciones óptimas que hagan más eficientes los recursos
	RFZ290	Error de administración	Débil gestión de contraseñas	Evitar el riesgo	Usar un sistema de gestión de contraseñas
	RFZ291	Error de actualización de Software	Software desfasado para la actualidad	Evitar el riesgo	Instalar un nuevo sistema operativo más actualizado
	RFZ292	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
	RFZ293	Aparición de virus o malware	Falta de programas antivirus/antimalware	Reducir el riesgo	Instalar un programa antivirus y antimalware
	RFZ294		Descargas de software no seguras.	Reducir el riesgo	Crear un plan de capacitación y concientización a usuarios
	RFZ295	Licencia ilegal de software	Ataques de tipo ransomware	Reducir el riesgo	Instalar un programa antivirus y antimalware, instalar una licencia original
MICROSOFT OFFICE 2013	RFZ296	Error de configuración	Configuración predeterminada no óptima para los equipos	Reducir el riesgo	Crear un plan de acción para crear configuraciones óptimas que hagan más eficientes los recursos
	RFZ297	Error de actualización de Software	Software desfasado para la actualidad	Evitar el riesgo	Instalar un nuevo procesador de textos más actualizado
	RFZ298	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
	RFZ299	Licencia ilegal de software	Ataques de tipo ransomware	Reducir el riesgo	Instalar un programa antivirus y antimalware, instalar una licencia original

MICROSOFT OFFICE 2016	RFZ300	Error de configuración	Configuración predeterminada no óptima para los equipos	Reducir el riesgo	Crear un plan de acción para crear configuraciones óptimas que hagan más eficientes los recursos
	RFZ301	Error de actualización de Software	Software desfasado para la actualidad	Evitar el riesgo	Instalar un nuevo procesador de textos más actualizado
	RFZ302	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
	RFZ303	Licencia ilegal de software	Ataques de tipo ransomware	Reducir el riesgo	Instalar un programa antivirus y antimalware, instalar una licencia original
SCRATCH V3	RFZ304	Error de configuración	Configuración predeterminada no óptima para los equipos	Reducir el riesgo	Capacitar a los usuarios a fin de orientar en la configuración óptima
	RFZ305	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
XMIND	RFZ306	Error de configuración	Configuración predeterminada no óptima para los equipos	Reducir el riesgo	Capacitar a los usuarios a fin de orientar en la configuración óptima
	RFZ307	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)

CMAPTOOLS	RFZ308	Error de configuración	Configuración predeterminada no óptima para los equipos	Reducir el riesgo	Capacitar a los usuarios a fin de orientar en la configuración óptima
	RFZ309	Borrar información	Falta de software administrador de núcleo (protección de partituras del disco)	Evitar el riesgo	Instalar un programa administrador de núcleo (DeepFreeze)
MODEM ROUTER	RFZ310	Fuego	No existe un extintor de fuego cerca al lugar de almacenamiento	Reducir el riesgo	Comprar extintor de incendios
	RFZ311	Rayo	No existe un pararrayos que proteja ante descargas eléctricas	Reducir el riesgo	Implementar un pararrayos básico en un lugar estratégico a fin de evitar descargas eléctricas a los equipos
	RFZ312	Polvo	Falta de limpieza constante del equipo	Evitar el riesgo	Crear una política de limpieza de los equipos
	RFZ313	Fallas en los equipos	No existe reemplazo inmediato del equipo	Asumir el riesgo	No se cuenta con un reemplazo del equipo, el router brindado está diseñado exclusivamente para la compañía que provee internet y por ende no puede ser reemplazado por un equipo similar
	RFZ314	Corte de energía	No existe UPS	Reducir el riesgo	Comprar un UPS
	RFZ315	Error de usuario	Manipulación inadecuada	Transferir el riesgo	Control de la configuración se encargará los técnicos de la compañía de internet

DOCENTES	RFZ316	Ingeniería social	Desconocimiento de tipos de ataques maliciosos	Reducir el riesgo	Crear capacitaciones y orientaciones
	RFZ317	Suplantación de identidad	Exceso de confianza	Reducir el riesgo	Crear políticas de control de accesos
	RFZ318	Acceso sin autorización	Descuido del personal de vigilancia	Reducir el riesgo	Crear políticas de control de accesos
PERSONAL ADMINISTRATIVO	RFZ319	Ingeniería social	Desconocimiento de tipos de ataques maliciosos	Reducir el riesgo	Crear capacitaciones y orientaciones
	RFZ320	Suplantación de identidad	Exceso de confianza	Reducir el riesgo	Crear políticas de control de accesos
	RFZ321	Acceso sin autorización	Descuido del personal de vigilancia	Reducir el riesgo	Crear políticas de control de accesos
	RFZ322	Personal no disponible	Falta de presupuesto para contratar personal calificado para el puesto	Transferir el riesgo	Ugel Huancayo debe garantizar el personal calificado
ESTUDIANTES	RFZ323	Mal uso de los recursos	Desconocimiento del uso de las laptops	Reducir el riesgo	Crear capacitaciones y orientaciones
	RFZ324	Mal uso del hardware	Maltrato a los equipos	Reducir el riesgo	Crear capacitaciones y orientaciones

Nota: Elaboración Propia, tipos de vulnerabilidades y acciones para abordar cada una de ellas.

3. VERIFICAR

Declaración de Aplicabilidad

TABLA XIV DECLARACIÓN DE APLICABILIDAD

ID	Control	Aplicabilidad	Justificación	Objetivos de control	Método de implementación	Estado
5	Políticas de seguridad de la información					
5.1	Directrices establecidas por la dirección para la seguridad de información					
5.1.1	Políticas para la seguridad de la información	SI	De suma importancia para controlar todos los demás riesgos	Dar a conocer a toda la comunidad educativa sobre las políticas de seguridad de la información	La alta dirección pública y divulga las políticas de seguridad de la información entre los miembros del personal y otras partes interesadas.	Completado
5.1.2	Revisión de las políticas para seguridad de la información	SI	De suma importancia para controlar todos los demás riesgos	Mantener en constante revisión las políticas de seguridad	Las políticas de seguridad de la información deben revisarse periódicamente de acuerdo con los procedimientos establecidos.	En proceso
6	Organización de la seguridad de la información					
6.1	Organización interna					
6.1.1	Roles y responsabilidades para la seguridad de información	SI	Dar a conocer los roles y responsabilidades a cada miembro	Tener claro cual son los roles y responsabilidades de cada participante de la institución	Las políticas de seguridad de la información deben seguirse a la hora de definir y asignar responsabilidades.	Completado
6.1.2	Separación de deberes	SI	Tener conocimiento de la organización	Lo mejor es dividir las tareas y las responsabilidades para evitar un mal uso de los recursos de la empresa.	Lo mejor es dividir las tareas y las responsabilidades para evitar un mal uso de los recursos de la empresa.	Completado
6.1.3	Contacto con las autoridades	NO	No representa un riesgo crítico para la Institución			

6.1.4	Contacto con grupos de interés especial	NO	No representa un riesgo crítico para la Institución			
6.1.5	Seguridad de la información en la gestión de proyectos	NO	No representa un riesgo crítico para la Institución			
7	Seguridad de los recursos humanos					
7.1	Antes de asumir el empleo.					
7.1.1	Selección	NO	No representa un riesgo crítico para la Institución			
7.1.2	Términos y condiciones del empleo	NO	No representa un riesgo crítico para la Institución			
7.2	Durante la ejecución del empleo					
7.2.1	Responsabilidades de la dirección	SI	RFZ06, RFZ94, RFZ97, RFZ102, RFZ119, RFZ121, RFZ124, RFZ127, RFZ129, RFZ145, RFZ181, RFZ192, RFZ195, RFZ201, RFZ223, RFZ275, RFZ294	Controlar a todo el personal a fin de que se logre cumplir con las políticas creadas	Se debe exigir a los empleados, contratistas y terceros el cumplimiento a cabalidad de las políticas de seguridad de la información implementada.	Completado
7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	SI	RFZ06, RFZ94, RFZ97, RFZ102, RFZ119, RFZ121, RFZ124, RFZ127, RFZ129, RFZ145, RFZ181, RFZ192, RFZ195, RFZ201, RFZ223, RFZ275, RFZ294	Se debe realizar una capacitación a todo el personal de manera conjunta respecto a temas de la seguridad de la información	Realizar capacitaciones periódicas a todo el personal de la institución	En proceso

7.2.3	Proceso disciplinario	NO	No representa un riesgo crítico para la Institución			
7.3	Terminación o cambio de empleo					
7.3.1	Terminación o cambio de responsabilidades de empleo	NO	No representa un riesgo crítico para la Institución			
8	Gestión de activos					
8.1	Responsabilidad por los activos					
8.1.1	Inventario de activos	SI	El inventario de la Institución es obsoleto y necesita actualización	Se debe contar con un inventario detallado de los activos que posee la Institución.	Elaborar y corroborar un inventario detallado de todos los activos de la institución	Completado
8.1.2	Propiedad de los activos	SI	Los propietarios de los activos no fueron actualizados	Se debe identificar al responsable de cada activo	Elaborar junto con el inventario una designación de un responsable	Completado
8.1.3	Uso aceptable de los activos	SI	RFZ06, RFZ07	Debe incluirse una disposición que obligue a los empleados a comprometerse a utilizar los recursos de la organización de forma adecuada.	Elaborar un documento de compromiso de cada empleado	En proceso

8.1.4	Devolución de activos	NO	No representa un riesgo crítico para la Institución	Los empleados que cambian de puesto o cuyos contratos se rescinden deben disponer de un procedimiento para la devolución de activos.	Elaborar una disposición de entrega y devolución de cada activo	
8.2	Clasificación de la información					
8.2.1	Clasificación de la información	NO	No es crítico para la seguridad			
8.2.2	Etiquetado de la información	NO	No es crítico para la seguridad			
8.2.3	Manejo de activos	NO	No es crítico para la seguridad			
8.3	Manejo de medios					
8.3.1	Gestión de medios removibles	NO	No representa un riesgo crítico para la Institución			
8.3.2	Disposición de los medios	NO	No representa un riesgo crítico para la Institución			
8.3.3	Transferencia de medios físicos	SI	RFZ257, RFZ261	Mantener los archivos y medio físicos seguros durante su transferencia	Establecer protocolos que garanticen que los datos que contienen no se filtran, alteran o eliminan.	Completado
9	Control de acceso					
9.1	Requisitos del negocio para control de acceso					
9.1.1	Política de control de acceso	SI	RFZ52, RFZ54, RFZ79, RFZ81, RFZ106	Tener el control de los accesos de los usuarios	Cree políticas que concedan acceso a los datos de acuerdo con los privilegios definidos en función de las funciones que desempeñan.	Completado
9.1.2	Política sobre el uso de los servicios de red	NO	No representa un riesgo crítico para la Institución			

9.2	Gestión de acceso de usuarios					
9.2.1	Registro y cancelación del registro de usuarios	NO	No representa un riesgo crítico para la Institución			
9.2.2	Suministro de acceso de usuarios	NO	No representa un riesgo crítico para la Institución			
9.2.3	Gestión de derechos de acceso privilegiado	NO	No representa un riesgo crítico para la Institución			
9.2.4	Gestión de información de autenticación secreta de usuarios	NO	No representa un riesgo crítico para la Institución			
9.2.5	Revisión de los derechos de acceso de usuarios	NO	No representa un riesgo crítico para la Institución			
9.2.6	Retiro o ajuste de los derechos de acceso	NO	No representa un riesgo crítico para la Institución			
9.3	Responsabilidades de los usuarios					
9.3.1	Uso de la información de autenticación secreta	SI	RFZ103, RFZ104	Asegurar el acceso a personas autorizadas	Se deben crear perfiles para acceder a la información considerada más importante para la empresa.	En proceso
9.4	Control de acceso a sistemas y aplicaciones					
9.4.1	Restricción de acceso Información	SI	RFZ103, RFZ104	Solo personal autorizado tiene acceso a cierto tipo de información	Limitar el acceso a la información por parte de personal no autorizado.	Completado
9.4.2	Procedimiento de ingreso seguro	SI	RFZ103, RFZ104	Solo personal autorizado tiene acceso a cierto tipo de información	Se deben establecer procedimientos que restrinjan el acceso a la información a personal no autorizado	Completado
9.4.3	Sistema de gestión de contraseñas	SI	RFZ52, RFZ79, RFZ106	Contraseñas seguras y gestionadas adecuadamente	Es importante establecer directrices de gestión de contraseñas, incluidas las relativas a la caducidad, el bloqueo tras varios intentos y los requisitos para crear contraseñas seguras.	Completado

9.4.4	Uso de programas utilitarios privilegiados	SI	RFZ43, RFZ49, RFZ50	Controlar el uso de diversos programas de origen desconocido	Limite el uso de programas de utilidades, ya que pueden comprometer la seguridad de la contraseña.	Completado
9.4.5	Control de acceso a códigos fuente de programas	NO	No representa un riesgo crítico para la Institución			
10	Criptografía					
10.1	Controles criptográficos					
10.1.1	Política sobre el uso de controles criptográficos	NO	No representa un riesgo crítico para la Institución			
10.1.2	Gestión de llaves	NO	No representa un riesgo crítico para la Institución			
11	Seguridad física y del entorno					
11.1	Áreas seguras					
11.1.1	Perímetro de seguridad física	NO	No representa un riesgo crítico para la Institución			
11.1.2	Controles físicos de entrada	SI	RFZ182, RFZ310	Controlar el acceso a los modems router y PCs administrativas	Se debe restringir el acceso a sitios seguros como centro de cableado, ubicación del servidor, espacios donde se encuentre información confidencial, estos sitios deben permanecer con llave.	Completado
11.1.3	Seguridad de oficinas, recintos e instalaciones	SI	RFZ08, RFZ09, RFZ15, RFZ16	Controlar el ingreso solo de personal autorizado	Restringir el acceso a personal no autorizado, las áreas deben estar demarcadas dando aviso que son sitios restringidos	Completado

11.1.4	Protección contra amenazas externas y ambientales	SI	RFZ01, RFZ02, RFZ09, RFZ12, RFZ13, RFZ172, RFZ164	Controlar los daños ocacionados por amenazas externas (rayos)	Se debe contar con detectores de humo y humedad, ubicación de extinguidores en sitios estratégicos, cuartos técnicos con aire acondicionado, adquisición de pólizas contra robo y desastres naturales	En proceso
11.1.5	Trabajo en áreas seguras	SI	RFZ01, RFZ02, RFZ09, RFZ12, RFZ13, RFZ172, RFZ164	Controlar el acceso a solo personal autorizado	Se deben preservar los sitios donde se encuentren activos valiosos con el fin de protegerlos contra daños intencionados	Completado
11.1.6	Áreas de despacho y carga	NO	No representa un riesgo crítico para la Institución			
11.2	Equipos					
11.2.1	Ubicación y protección de los equipos	SI	RFZ12, RFZ20, RFZ24, RFZ28, RFZ55	Protección de los equipos contra robo	Los equipos deben estar ubicados en sitios seguros, de esta forma se protege contra robo, accesos no autorizados.	Completado
11.2.2	Servicios de suministro	SI	RFZ05, RFZ33, RFZ60, RFZ87	Protección contra cortes de energía	Se debe contar con un adecuado suministro y respaldo de energía	Completado
11.2.3	Seguridad del cableado	NO	No representa un riesgo crítico para la Institución			
11.2.4	Mantenimiento de equipos	SI	RFZ07, RFZ45, RFZ46	Mantener los equipos de forma segura	Es necesario realizar un mantenimiento preventivo y correctivo a intervalos predeterminados para proteger las actualizaciones de hardware y software.	Completado
11.2.5	Retiro de activos	NO	No representa un riesgo crítico para la Institución			

11.2.6	Seguridad de equipos y activos fuera de las instalaciones	SI	RFZ80	Controlar el préstamo de equipos a docentes	Aplicar la misma seguridad que se realiza a los equipos dentro de la empresa	
11.2.7	Disposición segura o reutilización de equipos	NO	No representa un riesgo crítico para la Institución			
11.2.8	Equipos de usuario desatendidos	SI	RFZ42, RFZ69, RFZ96	Controlar la información de los usuarios	Establece normas para el equipo cuando los usuarios no estén para evitar robos de información o accesos ilegales.	Completado
11.2.9	Política de escritorio limpio y pantalla limpia	SI	RFZ03, RFZ14, RFZ22	Mantener limpios los equipos	Establece protocolos para mantener las mesas libres de papeles, dispositivos de almacenamiento que puedan provocar fugas de información y pautas de limpieza de pantallas.	Completado
12	Seguridad de las operaciones					
12.1	Procedimientos operacionales y responsabilidades					
12.1.1	Procedimientos de operación documentados	SI	RFZ07, RFZ45, RFZ74, RFZ99, RFZ101, RFZ128, RFZ168	Tener manuales de uso de equipos a disposición	Todos los procedimientos, incluidos los manuales de operaciones particulares, deben registrarse y ponerse a disposición de los usuarios.	Completado
12.1.2	Gestión de cambios	NO	No representa un riesgo crítico para la Institución			
12.1.3	Gestión de capacidad	NO	No representa un riesgo crítico para la Institución			
12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	NO	No representa un riesgo crítico para la Institución			
12.2	Protección contra códigos maliciosos					

12.2.1	Controles contra códigos maliciosos	SI	RFZ10, RFZ11, RFZ39, RFZ51, RFZ66, RFZ67, RFZ78, RFZ93, RFZ94, RFZ132, RFZ144, RFZ145	Antivirus que protege los equipos	El software, que protege los ordenadores contra códigos maliciosos y debe actualizarse con frecuencia para proporcionar parches que solucionen nuevas vulnerabilidades, es un requisito para los equipos informáticos.	Completado
12.3	Copias de respaldo					
12.3.1	Respaldo de información	SI	RFZ53, RFZ69, RFZ80, RFZ96, RFZ107, RFZ134, RFZ147, RFZ216, RFZ227, RFZ241, RFZ245, RFZ249, RFZ254, RFZ257, RFZ261, RFZ264, RFZ266	Respaldar la información	Deben realizarse pruebas para garantizar que los datos cumplen las políticas de copia de seguridad y que la información está respaldada.	Completado
12.4	Registro y seguimiento					
12.4.1	Registro de eventos	NO	No representa un riesgo crítico para la Institución			
12.4.2	Protección de la información de registro	NO	No representa un riesgo crítico para la Institución			
12.4.3	Registros del administrador y del operador	NO	No representa un riesgo crítico para la Institución			
12.4.4	sincronización de relojes	NO	No representa un riesgo crítico para la Institución			
12.5	Control de SOFTWARE. operacional					
12.5.1	Instalación de SOFTWARE. En sistemas operativos	SI	RFZ284, RFZ291, RFZ297, RFZ301	Solo personas autorizadas pueden realizar instalación de determinados programas.	Es necesario restringir la instalación de software, permitiendo que sólo las personas registradas a las que se haya concedido permiso lleven a cabo estas tareas.	Completado
12.6	Gestión de la vulnerabilidad técnica					

12.6.1	Gestión de las vulnerabilidades técnicas	SI	RFZ288, RFZ295, RFZ299	Minimizar las vulnerabilidades de los activos	Es importante poner en marcha procesos que reduzcan las vulnerabilidades a las que se enfrentan los activos tecnológicos.	Completado
12.6.2	Restricciones sobre la instalación de SOFTWARE.	SI	RFZ37, RFZ62, RFZ69, RFZ89, RFZ91, RFZ118, RFZ130, RFZ211	Solo instalar software necesario para el manejo de equipos	Es necesario restringir la instalación de software para que sólo las personas con permiso puedan llevar a cabo estas tareas, y esas personas deben estar registradas.	Completado
12.7	Consideraciones sobre auditorias de sistemas de información					
12.7.1	Información controles de auditoría de sistemas	NO	No representa un riesgo crítico para la Institución			
13	Seguridad de las comunicaciones					
13.1	Gestión de la seguridad de las redes					
13.1.1	Controles de redes	NO	No representa un riesgo crítico para la Institución			
13.1.2	Seguridad de los servicios de red	NO	No representa un riesgo crítico para la Institución			
13.1.3	Separación en las redes	NO	No representa un riesgo crítico para la Institución			
13.2	Transferencia de información					
13.2.1	Políticas y procedimientos de transferencia de información	NO	No representa un riesgo crítico para la Institución			
13.2.2	Acuerdos sobre transferencia de información	NO	No representa un riesgo crítico para la Institución			

13.2.3	Mensajería electrónica	SI	Difundir información falsa dentro de la comunidad educativa	Control de información compartida en la comunidad educativa	Establecer políticas sobre el uso adecuado de los recursos, en este caso utilizar el correo electrónico sólo para el desarrollo de las funciones asignadas. También deben instalarse programas que detecten spam y amenazas antivirus. Impartir formación sobre correos electrónicos sospechosos y cuentas falsas.	
13.2.4	Acuerdos de confidencialidad o de no divulgación	NO	No representa un riesgo crítico para la Institución			
14	Adquisición, desarrollo y mantenimientos de sistemas					
14.1	Requisitos de seguridad de los sistemas de información					
14.1.1	Análisis y especificación de requisitos de seguridad de la información	NO	No representa un riesgo crítico para la Institución			
14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	NO	No representa un riesgo crítico para la Institución			
14.1.3	Protección de transacciones de los servicios de las aplicaciones	NO	No representa un riesgo crítico para la Institución			
14.2	Seguridad en los procesos de desarrollo y soporte					
14.2.1	Política de desarrollo seguro	NO	No representa un riesgo crítico para la Institución			
14.2.2	Procedimientos de control de cambios en sistemas	NO	No representa un riesgo crítico para la Institución			
14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	NO	No representa un riesgo crítico para la Institución			

14.2.4	Restricciones en los cambios a los paquetes de SOFTWARE.	NO	No representa un riesgo crítico para la Institución			
14.2.5	Principios de construcción de sistemas seguros	NO	No representa un riesgo crítico para la Institución			
14.2.6	Ambiente de desarrollo seguro	NO	No representa un riesgo crítico para la Institución			
14.2.7	Desarrollo contratado externamente	NO	No representa un riesgo crítico para la Institución			
14.2.8	Pruebas de seguridad de sistemas	NO	No representa un riesgo crítico para la Institución			
14.2.9	Prueba de aceptación de sistemas	NO	No representa un riesgo crítico para la Institución			
14.3	Datos de prueba					
14.3.1	Protección de datos de prueba	NO	No representa un riesgo crítico para la Institución			
15	Relación con los proveedores					
15.1	Seguridad de la información en las relaciones con los proveedores					
15.1.1	Política de seguridad de la información para las relaciones con proveedores	NO	No representa un riesgo crítico para la Institución			
15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	NO	No representa un riesgo crítico para la Institución			
15.1.3	Cadena de suministro de tecnología de información y comunicación	NO	No representa un riesgo crítico para la Institución			
15.2	Gestión de la prestación de servicios con los proveedores					
15.2.1	Seguimiento y revisión de los servicios de los proveedores	NO	No representa un riesgo crítico para la Institución			
15.2.2	Gestión de cambios en los servicios de proveedores	NO	No representa un riesgo crítico para la Institución			

16	Gestión de incidentes de seguridad de la información					
16.1	Gestión de incidentes y mejoras en la seguridad de la información					
16.1.1	Responsabilidad y procedimientos	NO	No representa un riesgo crítico para la Institución			
16.1.2	Reporte de eventos de seguridad de la información	SI	Reporte de eventos	Controlar mediante un informe los eventos que ocurren	Para dejar constancia de la solución, hay que registrar los incidentes relacionados con la seguridad de la información y mantener un registro de los mismos.	Completado
16.1.3	Reporte de debilidades de seguridad de la información	NO				
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	NO	No representa un riesgo crítico para la Institución			
16.1.5	Respuesta a incidentes de seguridad de la información	SI	Mantener informes de los incidentes ocurridos	Controlar los incidentes	Establecer un proceso de atención a incidentes	En proceso
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	NO				
16.1.7	Recolección de evidencia	NO				
17	Aspectos de seguridad de la información de la gestión de continuidad de negocio					
17.1	Continuidad de seguridad de la información					
17.1.1	Planificación de la continuidad de la seguridad de la información	SI	RFZ05, RFZ33, RFZ60, RFZ87, RFZ322, RFZ324	Continuidad de operaciones	Crear políticas que permitan la continuidad de operaciones dentro de la Institución educativa	En proceso
17.1.2	Implementación de la continuidad de la seguridad de la información	NO	No representa un riesgo crítico para la Institución			
17.1.3	Verificación, revisión y evaluación de la continuidad	NO	No representa un riesgo crítico para la Institución			

	de la seguridad de la información					
17.2	Redundancias					
17.2.1	Disponibilidad de instalaciones de procesamiento de información.	NO	No representa un riesgo crítico para la Institución			
18	Cumplimiento					
18.1	Cumplimiento de requisitos legales y contractuales					
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	NO	No representa un riesgo crítico para la Institución			
18.1.2	Derechos de propiedad intelectual	NO	No representa un riesgo crítico para la Institución			
18.1.3	Protección de registros	NO	No representa un riesgo crítico para la Institución			
18.1.4	Privacidad y protección de datos personales	SI	RFZ317, RFZ320	Cumplir con las políticas de la protección de datos personales	Crear políticas de protección de datos personales	
18.1.5	Reglamentación de controles criptográficos	NO	No representa un riesgo crítico para la Institución			
18.2	Revisiones de seguridad de la información					
18.2.1	Revisión independiente de la seguridad de la información	NO				
18.2.2	Cumplimiento con las políticas y normas de seguridad	SI	Continuidad de operaciones	Verificar de manera periódica el cumplimiento de las normas y políticas	De acuerdo con sus respectivas áreas de responsabilidad, la dirección debe evaluar el cumplimiento de las normas de seguridad de la información establecidas.	En proceso
18.2.3	Revisión del cumplimiento técnico	SI	Continuidad de operaciones	Verificar la comprensión de la comprensión de las políticas	Es importante comprobar que todos los empleados comprenden y acatan las políticas de seguridad de la información.	En proceso

Nota: Elaboración Propia, basado en la ISO 27001.

5.2. Descripción de resultados

Gracias a sus inversiones en TIC, La Institución Educativa “Francisco de Zela”, cuenta con el apoyo y soporte para la gestión de su información y la administración de sus recursos, pero aún no se cuenta con políticas y procesos formalizados que fomenten el uso responsable de estas TIC y brinden control sobre la información que manejan. Por lo que los activos críticos se han utilizado como modelo para la implantación de la seguridad de la información y el objetivo de un buen sistema de gestión de la seguridad de la información (SGSI) debido a la información que manejan.

El análisis inferencial y descriptivo, se muestra a continuación con sus respectivos resultados basados en las fichas de registro y encuestas realizadas en el anexo 4.

5.2.1. Análisis descriptivo de la seguridad de la información

Según se muestra en la tabla 13, para el indicador de seguridad de la información, el valor que se promedió en la ficha de registro Pre test es de un 75% y el promedio Post test es de un 21.4%. Además, luego de aplicar una comparativa entre ambas fichas de registro, se obtuvo un valor mínimo de 50% y un valor máximo de 100% para la prueba Pre test y un valor mínimo de 0% y un valor máximo de 50% para la prueba Post test. Con esto se logra evidenciar la mejora en la seguridad de la información luego de aplicar el SGSI en la Institución.

TABLA XV. ANÁLISIS DESCRIPTIVO PRE Y POST TEST DE SEGURIDAD DE LA INFORMACIÓN

	Mínimo %	Máximo %	Promedio %
Seguridad de la Información_Pre	50	100	75
Seguridad de la Información_Post	0	50	21.4

Noat: Elaboración propia.

A continuación, se muestra la comparación en el manejo de la información pre y post al SGSI.

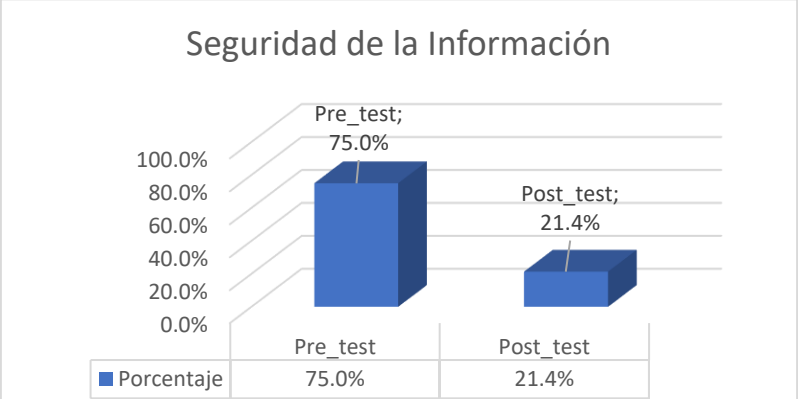

Fig. 12. Comparación entre Pre test y Post test de seguridad de la información

5.2.2. Análisis descriptivo del riesgo de la información

Según se muestra en la tabla 14, para el indicador de riesgo de la información, el valor que se promedió en la ficha de registro Pre test es de un 67.6% y el promedio Post test es de un 24.9%. Además, luego de aplicar una comparativa entre ambas fichas de registro, se obtuvo un valor mínimo de 50% y un valor máximo de 100% para la prueba Pre test y un valor mínimo de 0% y un valor máximo de 50% para la prueba Post test.

TABLA XVI. ANÁLISIS DESCRIPTIVO PRE Y POST TEST DE RIESGO DE LA INFORMACIÓN

	Mínimo %	Máximo %	Promedio %
Riesgo Información_Pre	50	100	67.6
Riesgo Información_Post	0	50	24.9

Nota: Elaboración propia.

Del mismo modo, en la figura 13 se puede apreciar la comparativa entre la prueba Pre y Post test de riesgo de la información, mostrando que, antes de implementar el SGSI más de la mitad de los encuestados tienen dudas respecto a los riesgos de la información y luego esto disminuye drásticamente una vez implementado el SGSI.

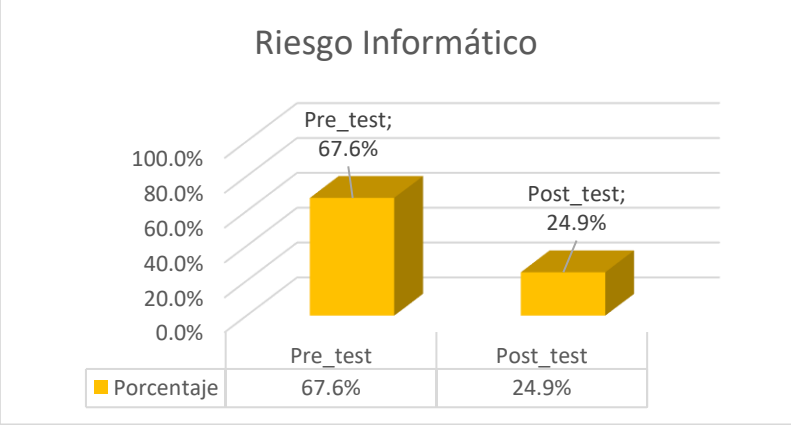

Fig. 13.Comparación entre Pre y Post test de riesgo informático

5.2.3. Análisis descriptivo del control informático

Según se muestra en la tabla 15, para el indicador de control informático, el valor que se promedió en la ficha de registro Pre test es de un 71.3% y el promedio Post test es de un 15.5%. Además, luego de aplicar una comparativa entre ambas fichas de registro, se obtuvo un valor mínimo de 50% y un valor máximo de 100% para la prueba Pre test y un valor mínimo de 0% y un valor máximo de 50% para la prueba Post test.

TABLA XVII. ANÁLISIS DESCRIPTIVO PRE Y POST TEST DE CONTROL INFORMÁTICO

	Mínimo %	Máximo %	Promedio %
Control Informático_Pre	50	100	71.3
Control Informático_Post	0	50	15.5

Nota: Elaboración propia.

Asimismo, la comparativa entre el Pre y Post test de las fichas de registro quedan mostradas en la siguiente figura:

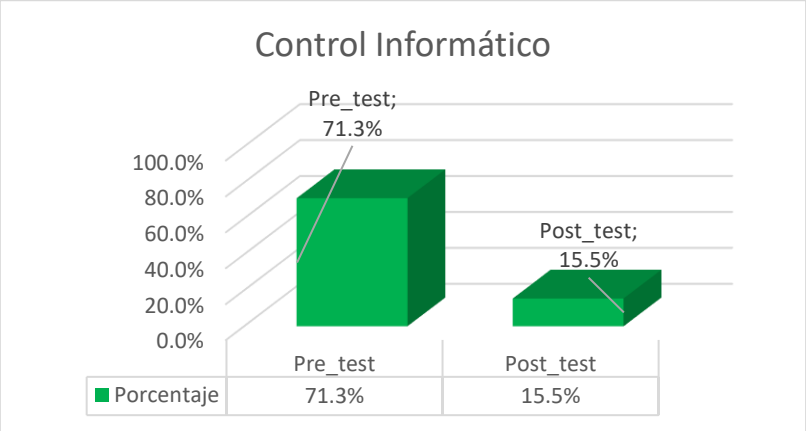

Fig. 14. Comparación entre Pre y Post test de control informático

5.2.4. Resultados de la Variable Dependiente

Ahora veamos los resultados obtenidos de la variable dependiente distribuidos de acuerdo a las dimensiones establecidas en la matriz de operalización de variables.

Dimensión "Seguridad de la Información"

Pregunta N°01: ¿El nivel de actualizaciones de seguridad, soluciones antivirus y antimalware son óptimos para trabajar en la institución?

El objetivo que se planteó con esta pregunta es saber en nivel de seguridad de los equipos con los que se opera dentro de la Institución educativa.

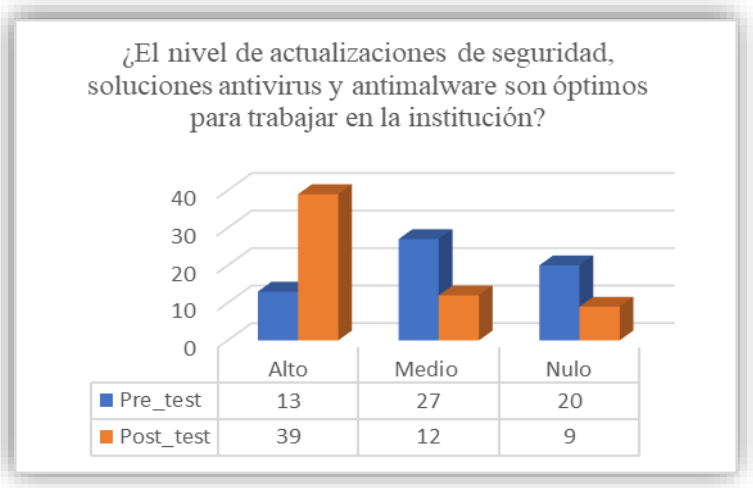

Fig. 15. Nivel de seguridad de equipos

Se puede distinguir, que en la prueba Pre test realizada a los encuestados, solo 13 de ellos mencionaron que el nivel de seguridad de los equipos era alto a comparación de los resultados Post test donde hubo una clara mejoría en las respuestas, obteniendo 39 respuestas a favor de un nivel alto en seguridad de los equipos. Si traducimos esto a números porcentuales, significaría un 21.7% de encuestados mencionando que la seguridad de los equipos está en un nivel alto antes de realizar la implementación del SGSI y luego este número sube a un 65% gracias a las políticas de seguridad planteadas y al trabajo de concientización del buen uso de los equipos. De igual manera, haciendo una comparativa de los resultados pre y post test respecto al nivel medio, se observa que 27 usuarios optaban por marcar esta respuesta antes de aplicar las recomendaciones de la norma ISO/IEC 27000, ahora luego de aplicar las recomendaciones se ve disminuida esa respuesta a solo 12 usuarios donde queda demostrado, que sus respuestas fueron a favor de la opción de un nivel alto.

También podemos apreciar estos valores en datos porcentuales para obtener una visión más holística de los resultados:

TABLA XVIII. INDICADOR DE NIVEL DE SEGURIDAD DE EQUIPOS.

	Nivel Alto %	**Nivel Medio %**	**Nivel Nulo %**
Pre test	21.7	45	33.3
Post test	65	20	15

Nota: Elaboración Propia.

Pregunta N°02: ¿Se almacena y gestiona las contraseñas de forma segura?

La finalidad de esta pregunta es saber el nivel de manejo de las políticas de gestión de contraseñas. Algo muy esencial hoy en día para controlar la seguridad en las cuentas institucionales y privadas de cada usuario del colegio.

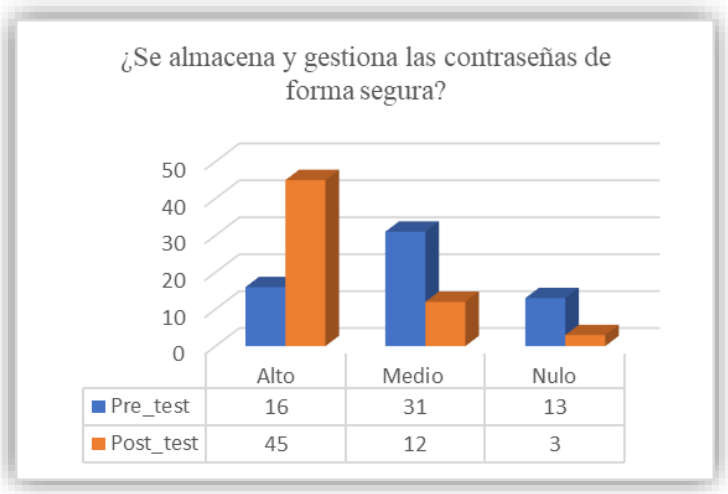

Fig. 16. Nivel de políticas de gestión de contraseñas.

Fuente, Elaboración Propia.

En el gráfico podemos apreciar que el nivel alto en la prueba Pre test era solo respondido por 16 de los 60 encuestados y luego de aplicar las políticas de gestión de contraseñas, asegurando reglas claras para la creación de contraseñas, como: longitud mínima, adición de caracteres especiales y elaborando un plan de capacitación con el uso de un programa gestor de contraseñas "Bitwarden" se logró que en la prueba Post test la respuesta a un nivel alto sea de 45 de 60 encuestados lo cual nos da un porcentaje del 75% de satisfacción de los usuarios. De igual manera al hacer una comparativa entre las respuestas de nivel medio y nulo podemos apreciar valores de 51.7% pre test y luego 20% post test para el nivel medio y en el nivel nulo valores de 21.7% pre test y 5% para el post test, lo cual nos dice que la brecha de desconocimiento de una política clara para la gestión de contraseñas queda en un margen mínimo. Para más detalle se observa la siguiente tabla:

TABLA XIX. INDICADOR NIVEL DE POLÍTICAS DE GESTIÓN DE CONTRASEÑAS.

	Nivel Alto %	**Nivel Medio %**	**Nivel Nulo %**
Pre test	26.7	51.7	21.7
Post test	75	20	5

Pregunta N°03: ¿Se registran y monitorean intentos de acceso no autorizados?

El objetivo con esta pregunta es saber el nivel con el cual se manejan las políticas de control de accesos en la institución, existen o no dichas políticas y como se puede ayudar a mejorar los accesos no autorizados.

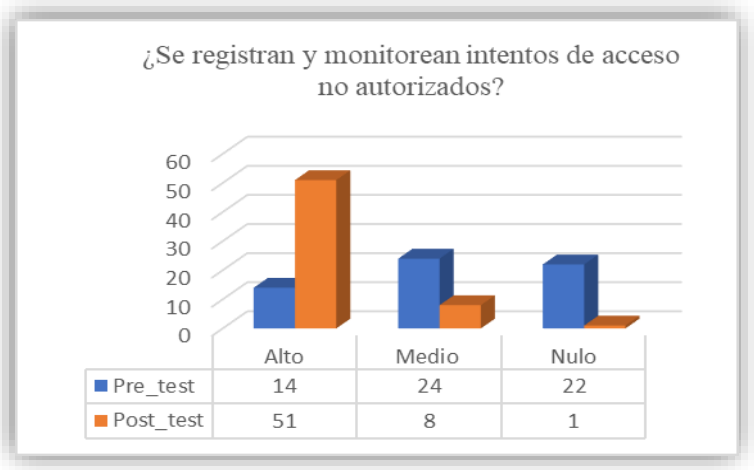

Fig. 17. Nivel de políticas de control de accesos

Fuente, Elaboración Propia.

Se puede apreciar la diferencia amplia que existe entre los resultados pre test y post test para el nivel alto de la pregunta, indicando a 14 participantes respondiendo sobre el conocimiento de registros y monitorización antes de aplicar la implementación de este trabajo de investigación y luego un gran aumento a 51 participantes mostrando la conformidad de obtener un nivel alto en dichos registros y accesos no autorizados. Para tener una visión más clara de estos datos nos basamos en la tabla N°18 donde podemos apreciar que solo un 23.3% de los encuestados conocían sobre una política de control de accesos antes de aplicar el SGSI, el otro 40 % aceptaba un nivel medio de control de accesos y el 36.7% mencionaba que no existe dicha política dentro de la Institución educativa, estos datos cambian drásticamente luego de la implementación de las políticas y procedimientos establecidos en el colegio, donde ahora se aprecia un 85% de usuarios consientes de la existencia de una política clara y establecida y solo un 1.7% de participantes aun no teniendo en claro la existencia de dicha política.

TABLA XX. INDICADOR DE NIVEL DE POLÍTICAS DE CONTROL DE ACCESOS.

	Nivel Alto %	**Nivel Medio %**	**Nivel Nulo %**
Pre test	23.3	40	36.7
Post test	85	13.3	1.7

Pregunta N°04: ¿En qué nivel se encuentran dividas las funciones y responsabilidades a fin de reducir los cambios sin autorización o el uso indebido de información o servicios?

La finalidad de esta pregunta es ver en qué nivel se encuentran divididas las funciones y responsabilidades de los actores de la Institución Educativa.

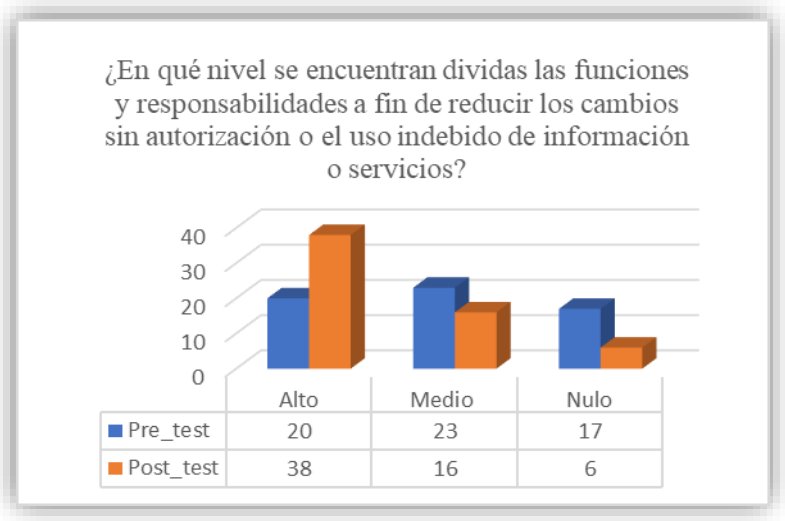

Fig. 18. Nivel de Segregación de funciones y responsabilidades

Apreciando la figura N°18 encontramos detalles interesantes como el hecho, de que en la prueba pre test existe una equivalencia entre los tres niveles de respuestas, esto nos indica la gran confusión que se tiene respecto a este tema. Luego de aplicar las pautas que nos menciona la ISO/IEC 27000, se establecieron responsables para cada uno de los activos críticos de la institución, con el fin de reducir el riesgo de omisión de funciones.

Si fijamos nuestra mirada a la tabla N°19, apreciamos como el porcentaje de nivel alto para este indicador sube de un 33.3% de encuestados a un 63.3% y el desconocimiento que se traduce como la respuesta hacia un nivel nulo disminuye de un 28.3% a solo un 10% del total de encuestados, lo ideal es en un futuro alcanzar un resultado en el nivel nulo del 0% pero cabe mencionar que esto depende mucho de la mejora continua que se aplica en un futuro a la implementación del SGSI.

TABLA XXI. INDICADOR DE NIVEL DE SEGREGACIÓN DE FUNCIONES Y RESPONSABILIDADES

	Nivel Alto %	**Nivel Medio %**	**Nivel Nulo %**
Pre test	33.3	38.3	28.3
Post test	63.3	26.7	10

Pregunta N°05: ¿Se tienen políticas de acceso físico y procedimientos establecidos para la gestión de incidentes de seguridad?

Lo que se busca con esta pregunta es analizar el nivel de aseguramiento de los accesos físicos en la Institución, se cumple o no con los ingresos autorizados de acuerdo a sus responsabilidades y funciones.

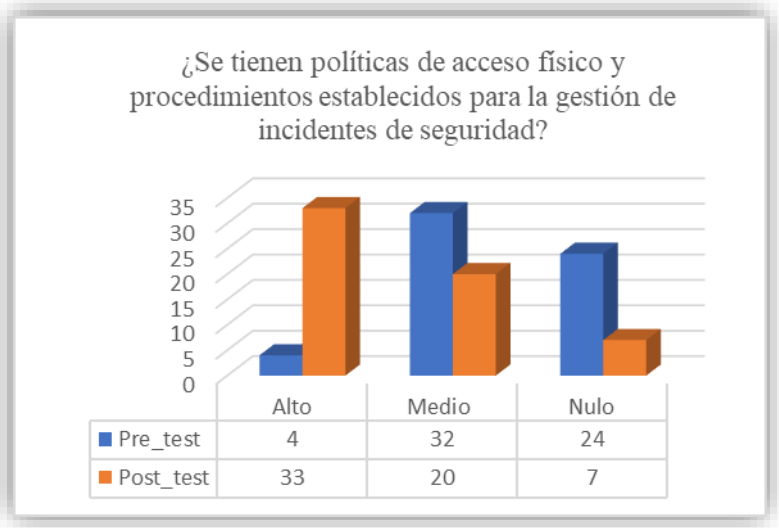

Fig. 19. Nivel de aseguramiento de controles de seguridad.

Fuente, Elaboración Propia.

TABLA XXII. INDICADOR DE NIVEL DE ASEGURAMIENTO DE CONTROLES DE SEGURIDAD.

	Nivel Alto %	Nivel Medio %	Nivel Nulo %
Pre test	6.7	53.3	40
Post test	55	33.3	11.7

Observando tanto la figura N°19 y la tabla N°20, distinguimos que el 40% de encuestados menciona no conocer ningún tipo de procedimiento para la gestión de incidentes, es más, desconocía el término. Al finalizar la prueba Post test se aprecia una gran diferencia respecto al desconocimiento de una buena gestión de incidentes, el cual nos permite asegurar que los controles de seguridad estén siendo procesados y monitoreados constantemente a fin de reducir los riesgos que se presenten en la Institución. De igual modo, se observa como el nivel alto de este indicador pasa de apenas un 6.7% a un 55% de encuestados, demostrando que más de la mitad de ellos se sienten conformes con el SGSI implementado.

Pregunta N°06: ¿En qué escala, existe un procedimiento para garantizar que al término del vínculo laboral los usuarios sean deshabilitados de todos los accesos informáticos?

El objetivo de esta pregunta es evaluar el nivel con que se manejan los procedimientos para deshabilitar los accesos a usuarios que ya no estén inmersos dentro de la institución educativa.

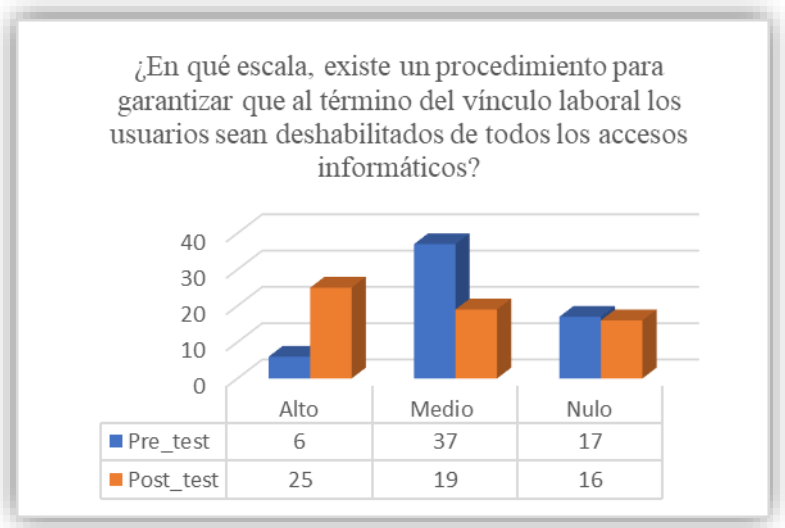

Fig. 20. Nivel de procedimientos para deshabilitar accesos.

TABLA XXIII. INDICADOR DE NIVEL DE PROCEDIMIENTOS PARA DESHABILITAR ACCESOS.

	Nivel Alto %	Nivel Medio %	Nivel Nulo %
Pre test	10	61.7	28.3
Post test	41.7	31.7	26.7

Se observa en la figura N°20 las respuestas de cada uno de los encuestados para los tres niveles propuestos y en la tabla N°21 los mismos resultados, pero en este caso traducidos a porcentajes para tener una visión más holística de cómo se van manejando las preguntas. Fijando nuestra mirada hacia los datos porcentuales apreciamos que: el 28.3% de los encuestados desconocían de dicho procedimiento y luego de la implementación del SGSI aún se mantiene un desconocimiento importante con un 26.7%, esto nos indica que, debemos hacer una nueva iteración de las políticas implementadas para mejorar en este aspecto y disminuir el grado de desconocimiento, también los nuevos planes de capacitación deben incluir este punto para brindar mayor claridad y despejar dudas.

Dimensión "Riesgo de la información"

Pregunta N°07: ¿Se realiza un seguimiento de la aceptación y cumplimiento del acuerdo de seguridad por parte de los usuarios?

La finalidad de esta pregunta es medir el nivel de aceptación de acuerdos por parte de los stakeholders de la Institución Educativa.

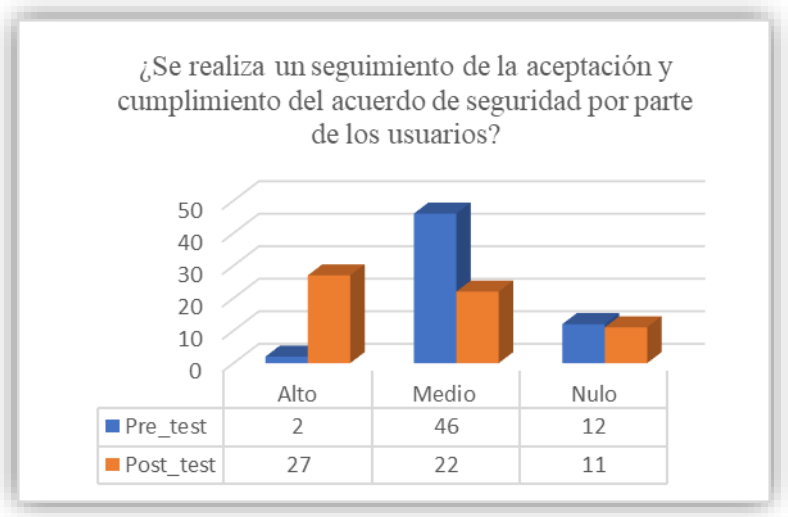

Fig. 21. Nivel de aceptación de acuerdos

TABLA XXIV. INDICADOR DE NIVEL DE ACEPTACIÓN DE ACUERDOS.

	Nivel Alto %	Nivel Medio %	Nivel Nulo %
Pre test	3.3	76.7	20
Post test	45	36.7	18.3

El porcentaje de nivel alto para esta pregunta según la prueba pre test, fue de apenas 3.3% demostrando que en su gran mayoría los encuestados no sentían que este indicador este presente dentro de la institución, según sus versiones, no se hace un seguimiento de los acuerdos establecidos y los monitoreos de los anteriores CIST (Coordinador de innovación y soporte tecnológico) solo eran básicos y referentes solo a las laptops del aula de innovación. Una vez implementado las políticas de seguridad, los usuarios mencionan que ahora se hace un seguimiento más amplio de los acuerdos y se monitorean todos los ambientes con los activos críticos mencionados en esta investigación.

Pregunta N°08: ¿Existe un procedimiento para destruir los datos obsoletos o inútiles?

El objetivo de esta pregunta es saber si se realizan procedimientos para eliminar datos que ya no son utilizados en la institución, tales como: registros de hace más de una década,

memorándums de años anteriores, trabajos de estudiantes que ya terminaron de estudiar en la institución, etc.

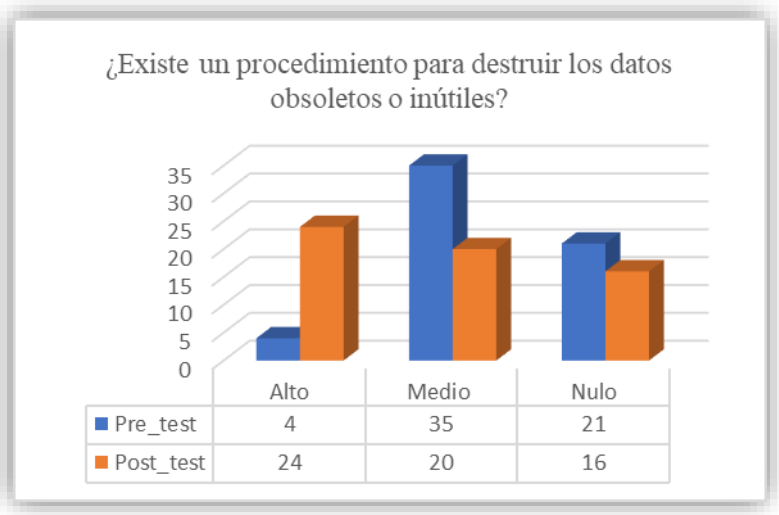

Fig. 22. Nivel de existencia de procedimientos de destrucción.

TABLA XXV. INDICADOR DE NIVEL DE EXISTENCIA DE PROCEDIMIENTOS DE DESTRUCCIÓN.

	Nivel Alto %	**Nivel Medio %**	**Nivel Nulo %**
Pre test	6.7	58.3	35
Post test	40	33.3	26.7

La tabla N°23 nos muestra dos datos importantes para analizar, lo primero es la diferencia marcada que existe entre la prueba pre test y post test para el nivel alto, indicando un 6.7% antes de implementar las medidas y procedimientos sugeridos y luego un 40%. Ahora respecto al nivel nulo de conocimiento de procedimientos de destrucción que se aplican en la institución, la diferencia no es muy amplia entre las dos pruebas realizadas, demostrando que aún existe trabajo por hacer para mejorar la percepción de los usuarios.

Pregunta N°09: ¿El nivel de seguridad de las copias de respaldo son los óptimos para proteger los datos y documentos contra, destrucción, perdida, falsificación, accesos y divulgación no autorizada?

Lo que se sugiere con esta pregunta es saber, de qué manera, se realizan los procedimientos de backups para proteger los activos de información de la institución educativa.

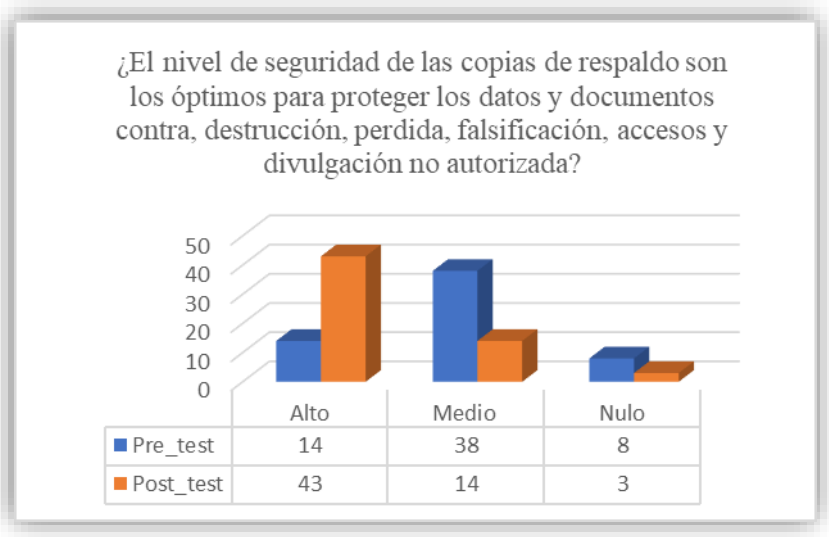

Fig. 23. Nivel de protección de datos.

TABLA XXVI. INDICADOR DE NIVEL PROTECCIÓN DE DATOS.

	Nivel Alto %	Nivel Medio %	Nivel Nulo %
Pre test	23.3	63.3	13.3
Post test	71.7	23.3	5

La figura N°23 nos muestra las respuestas obtenidas por los encuestados, donde queda en evidencia que el nivel nulo para esta pregunta es muy bajo antes y después de la implementación del SGSI mostrando solo 8 y 3 respuestas respectivamente. Ahora viendo la tabla N°24, observamos que la implementación de las políticas de respaldo, surgen con un buen porcentaje del 71.7% del total de encuestados. El nivel alto en la prueba post test nos demuestra la eficiencia y la importancia de aplicar de manera correcta los diferentes medios para respaldar la información importante del colegio.

Pregunta N°10: ¿Se maneja una política de escritorio limpio a fin de evitar divulgación de datos confidenciales?

La pregunta busca medir el nivel de continuidad operativa respecto a tener todos los datos confidenciales guardados y protegidos contra la usurpación de identidad y descuido del usuario.

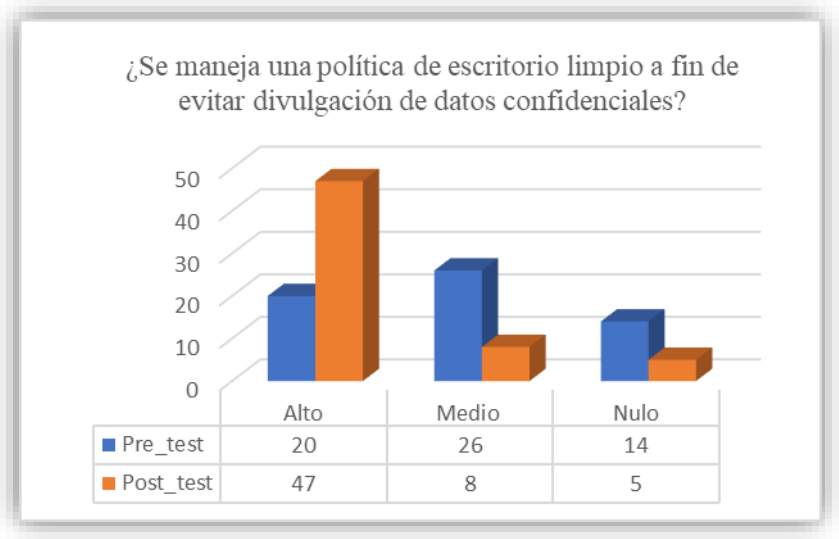

Fig. 24. Nivel de planes para la continuidad operativa.

TABLA XXVII. INDICADOR DE NIVEL DE PLANES PARA LA CONTINUIDAD OPERATIVA.

	Nivel Alto %	Nivel Medio %	Nivel Nulo %
Pre test	33.3	43.3	23.3
Post test	78.3	13.3	8.3

Si nos centramos en la tabla N°25, se aprecia que el porcentaje de nivel alto para este indicador obtiene un 78.3% para la prueba post test, esto quiere decir que se han aplicado de manera adecuada las recomendaciones que nos brinda la metodología utilizada, los encuestados sienten que ahora si la institución puede estar preparada para mantener sus operaciones en constante ritmo sin temor a las amenazas como: pérdida del fluido eléctrico, averías en las computadoras, olvido de contraseñas, divulgación de datos, etc.

Dimensión "Control Informático"

Pregunta N°11: ¿Se proporciona capacitaciones en seguridad de la información a todos los usuarios de los equipos informáticos de la Institución?

El objetivo de esta pregunta es saber el nivel con que se encuentran las capacitaciones sobre seguridad de información en la Institución educativa.

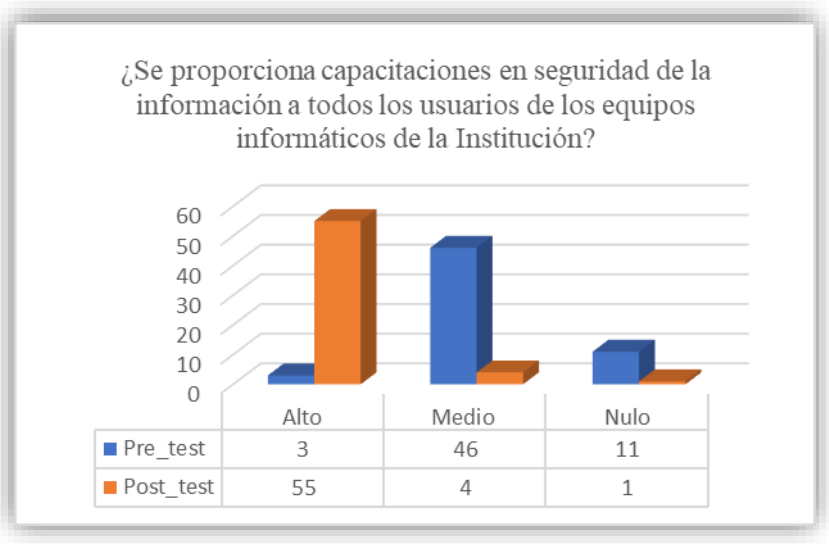

Fig. 25. Nivel de capacitaciones de seguridad de la información.

TABLA XXVIII. INDICADOR DE NIVEL DE CAPACITACIONES DE SEGURIDAD DE LA INFORMACIÓN

	Nivel Alto %	Nivel Medio %	Nivel Nulo %
Pre test	5	76.7	18.3
Post test	91.7	6.7	1.7

La figura N°25 nos muestra como el nivel alto de este indicador, sube drásticamente luego de implementar el SGSI en la institución educativa "Francisco de Zela". Por su parte la tabla N°26 nos muestra el porcentaje de respuestas para esta pregunta, indicando que, de solo tener un 5% de encuestados mencionando que no se realizaba capacitaciones a un nivel alto dentro de la institución, se pasa a tener un 91.7% de encuestados mencionando que ahora si se realizan capacitaciones periódicas orientadas a la seguridad de la información.

Pregunta N°12: ¿Se elabora un plan de concientización respecto a temas de seguridad de la información?

La finalidad de esta pregunta es tener en claro si se realiza un plan de concientización sobre temas relacionas a la seguridad de la información.

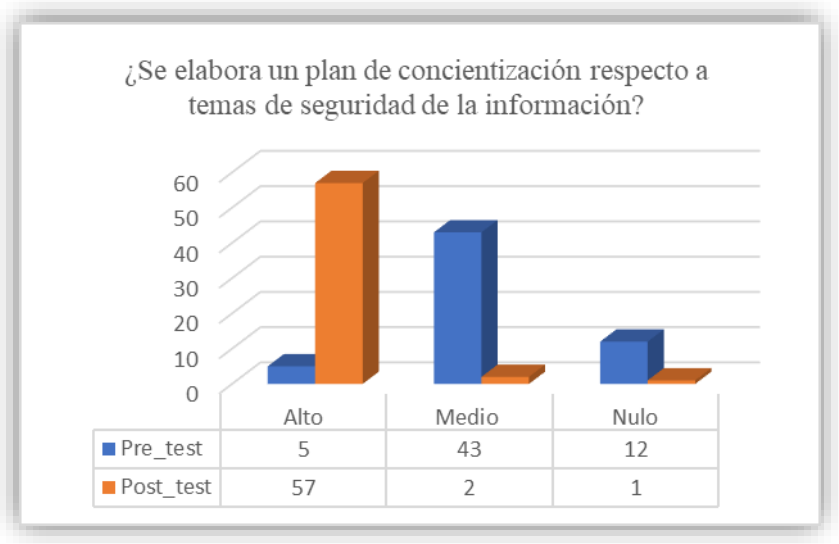

Fig. 26. Nivel de concientización de la seguridad de la información.

TABLA XXIX. INDICADOR DE NIVEL DE CONCIENTIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

	Nivel Alto %	Nivel Medio %	Nivel Nulo %
Pre test	8.3	71.7	20
Post test	95	3.3	1.7

En la tabla N°27 se puede apreciar a un 20% de encuestados que desconocían de la existencia de un plan de concientización sobre seguridad de la información. Luego de implementar medidas de concientización, como el uso adecuado de los equipos tecnológicos, no abrir páginas web sospechosas, tener diferentes contraseñas para cada una de las cuentas que se manejan y ayudarse de un gestor de contraseñas, el resultado que nos muestra la prueba Post test es que el nivel de desconocimiento se redujo a un 1.7% del total de encuestados. Por otro lado, el nivel alto de satisfacción con las medidas de concientización sube de un 8.3% a un 95% de encuestados, demostrando que se hace efectivo las recomendaciones de la ISO/IEC 27000.

5.3. Contrastación de Hipótesis

5.3.1. Hipótesis Específica 01

El sistema de gestión de la seguridad de la información favorece significativamente la seguridad de información de la I.E. Francisco de Zela.

A. Prueba de normalidad

Formulamos H_0 y H_1:

H_0: Los datos de la variable tienen una distribución normal.

H_1: Los datos de la variable NO tienen una distribución normal.

TABLA XXX. PRUEBA DE NORMALIDAD PARA HIPÓTESIS ESPECÍFICA 01

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
pre_test	,211	16	,054	,886	16	,048
post_test	,287	16	,001	,793	16	,002

a. Corrección de significación de Lilliefors

B. Regla de decisión

Si p<0,05 rechazamos la H_0 y aceptamos la H_1.

Si p>=0,05 rechazamos la H_1 y aceptamos la H_0.

Conclusión:

El valor de p, tanto para la prueba pre test y post test es menor a 0,05. Como se muestra en la tabla N°28 en la prueba de normalidad Shapiro-Wilk, el nivel de significación es de 0,048 para el pre test y 0,002 para el post test, aceptando la H_1 y rechazando la H_0. Por tanto, la distribución de los datos no es normal y aplicaremos las pruebas no paramétricas.

Prueba no paramétrica de Wilcoxon

Paso 1: Formulación de H_0 y H_1:

H_0: El sistema de gestión de la seguridad de la información no favorece significativamente la seguridad de información de la I.E. Francisco de Zela.

H_1: El sistema de gestión de la seguridad de la información favorece significativamente la seguridad de información de la I.E. Francisco de Zela.

Paso 2: Nivel de significancia α = 0,05 = 5%.

Paso 3: Se elije la prueba no paramétrica de Wilcoxon por ser datos no normales.

Paso 4: Regla de decisión

TABLA XXXI. CÁLCULO DE LA PRUEBA WILCOXON PARA HIPÓTESIS ESPECÍFICA 1

Descriptivos

			Estadístico	Desv. Error
Pre_test	Media		75,13	3,642
	95% de intervalo de confianza para la media	Límite inferior	67,36	
		Límite superior	82,89	
	Media recortada al 5%		75,14	
	Mediana		71,00	
	Varianza		212,250	
	Desv. Desviación		14,569	
	Mínimo		50	
	Máximo		100	
	Rango		50	
	Rango intercuartil		13	
	Asimetría		,591	,564
	Curtosis		-,110	1,091
Post_test	Media		21,25	5,142
	95% de intervalo de confianza para la media	Límite inferior	10,29	
		Límite superior	32,21	
	Media recortada al 5%		20,83	
	Mediana		29,00	
	Varianza		423,000	
	Desv. Desviación		20,567	
	Mínimo		0	
	Máximo		50	
	Rango		50	
	Rango intercuartil		33	
	Asimetría		,108	,564
	Curtosis		-1,720	1,091

TABLA XXXII. RESUMEN DE PRUEBA WILCOXON PARA HIPÓTESIS ESPECÍFICA 1.

Resumen de prueba de hipótesis

	Hipótesis nula	Prueba	Sig.	Decisión
1	La mediana de las diferencias entre pre_test y post_test es igual a 0.	Prueba de rangos con signo de Wilcoxon para muestras relacionadas	,001	Rechazar la hipótesis nula.

Se muestran significaciones asintóticas. El nivel de significación es de ,05.

Si el P-valor ≥ 0,05, se acepta H_0

Si el P-valor < 0,05, se acepta H_1

Paso 5: Conclusión

P-valor = 0,001 < α = 0,05

Hay una diferencia significativa en la seguridad de la información entre la prueba pre test (antes) y post test (después) de la implementación de sistema de gestión de seguridad de la información. Así se concluye el P-valor es menor a 0,05 y se acepta la H_1, es decir: El sistema de gestión de la seguridad de la información favorece significativamente la seguridad de información de la I.E. Francisco de Zela, con un valor porcentual del 95% de confianza.

5.3.2. Hipótesis Específica 02

El sistema de gestión de la seguridad de la información favorece significativamente la gestión de riesgos de la información de la I.E. Francisco de Zela.

A. Prueba de normalidad

Formulamos H_0 y H_1:

H_0: Los datos de la variable tienen una distribución normal.

H_1: Los datos de la variable NO tienen una distribución normal.

TABLA XXXIII. PRUEBA DE NORMALIDAD PARA HIPÓTESIS ESPECÍFICA 2

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Pre_test	,288	16	,001	,825	16	,006
Post_test	,201	16	,083	,834	16	,008

a. Corrección de significación de Lilliefors

B. Regla de decisión

Si p<0,05 rechazamos la H_0 y aceptamos la H_1.

Si p>=0,05 rechazamos la H_1 y aceptamos la H_0.

Conclusión:

El valor de p, tanto para la prueba pre test y post test es menor a 0,05. Como se muestra en la tabla N°31 en la prueba de normalidad Shapiro-Wilk, el nivel de significación es de 0,006 para el pre test y 0,008 para el post test, aceptando la H_1 y rechazando la H_0. Por tanto, la distribución de los datos no es normal y aplicaremos las pruebas no paramétricas.

Prueba no paramétrica de Wilcoxon

Paso 1: Formulación de H_0 y H_1:

H_0: El sistema de gestión de la seguridad de la información no favorece significativamente la gestión de riesgos de la información de la I.E. Francisco de Zela.

H_1: El sistema de gestión de la seguridad de la información favorece significativamente la gestión de riesgos de la información de la I.E. Francisco de Zela.

Paso 2: Nivel de significancia $\alpha = 0,05 = 5\%$.

Paso 3: Se elije la prueba no paramétrica de Wilcoxon por ser datos no normales.

Paso 4: Regla de decisión

TABLA XXXIV. CÁLCULO DE LA PRUEBA WILCOXON PARA LA HIPÓTESIS ESPECÍFICA 2

Descriptivos

			Estadístico	Desv. Error
Pre_test	Media		67,7500	3,09771
	95% de intervalo de confianza para la media	Límite inferior	61,1474	
		Límite superior	74,3526	
	Media recortada al 5%		66,9444	
	Mediana		67,0000	
	Varianza		153,533	
	Desv. Desviación		12,39086	
	Mínimo		50,00	
	Máximo		100,00	
	Rango		50,00	
	Rango intercuartil		4,50	
	Asimetría		,834	,564
	Curtosis		2,366	1,091
Post_test	Media		24,8750	5,14933
	95% de intervalo de confianza para la media	Límite inferior	13,8995	
		Límite superior	35,8505	
	Media recortada al 5%		24,8611	
	Mediana		25,0000	
	Varianza		424,250	
	Desv. Desviación		20,59733	
	Mínimo		,00	
	Máximo		50,00	
	Rango		50,00	
	Rango intercuartil		50,00	
	Asimetría		,023	,564
	Curtosis		-1,543	1,091

TABLA XXXV. RESUMEN DE PRUEBA WILCOXON PARA HIPÓTESIS ESPECÍFICA 2

Resumen de prueba de hipótesis

	Hipótesis nula	Prueba	Sig.	Decisión
1	La mediana de las diferencias entre Pre_test y Post_test es igual a 0.	Prueba de rangos con signo de Wilcoxon para muestras relacionadas	,000	Rechazar la hipótesis nula.

Se muestran significaciones asintóticas. El nivel de significación es de ,05.

Si el P-valor ≥ 0,05, se acepta H_0

Si el P-valor < 0,05, se acepta H_1

Paso 5: Conclusión

P-valor = 0,000 < α = 0,05

Hay una diferencia significativa en la seguridad de la información entre la prueba pre test (antes) y post test (después) de la implementación de sistema de gestión de seguridad de la información. Así se concluye el P-valor es menor a 0,05 y se acepta la H_1, es decir: El sistema de gestión de la seguridad de la información favorece significativamente la gestión de riesgos de información de la I.E. Francisco de Zela, con un valor porcentual del 95% de confianza.

5.3.3. Hipótesis Específica 03

El sistema de gestión de la seguridad de la información favorece significativamente el control informático de la I.E. Francisco de Zela.

A. Prueba de normalidad

Formulamos H_0 y H_1:

H_0: Los datos de la variable tienen una distribución normal.

H_1: Los datos de la variable NO tienen una distribución normal.

TABLA XXXVI. PRUEBA DE NORMALIDAD PARA HIPÓTESIS ESPECÍFICA 3

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Pre_test	,158	14	,200*	,874	14	,048
Post_test	,354	14	,000	,750	14	,001

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

B. Regla de decisión

Si p<0,05 rechazamos la H_0 y aceptamos la H_1.

Si p>=0,05 rechazamos la H_1 y aceptamos la H_0.

Conclusión:

El valor de p, tanto para la prueba pre test y post test es menor a 0,05. Como se muestra en la tabla N°34 en la prueba de normalidad Shapiro-Wilk, el nivel de significación es de 0,048 para el pre test y 0,001 para el post test, aceptando la H_1 y rechazando la H_0. Por tanto, la distribución de los datos no es normal y aplicaremos las pruebas no paramétricas.

Prueba no paramétrica de Wilcoxon

Paso 1: Formulación de H_0 y H_1:

H_0: El sistema de gestión de la seguridad de la información no favorece significativamente el control informático de la I.E. Francisco de Zela.

H_1: El sistema de gestión de la seguridad de la información favorece significativamente el control informático de la I.E. Francisco de Zela.

Paso 2: Nivel de significancia $\alpha = 0,05 = 5\%$.

Paso 3: Se elije la prueba no paramétrica de Wilcoxon por ser datos no normales.

Paso 4: Regla de decisión

TABLA XXXVII. CÁLCULO DE LA PRUEBA WILCOXON PARA HIPÓTESIS ESPECÍFICA 3

Descriptivos

			Estadístico	Desv. Error
Pre_test	Media		71,36	5,009
	95% de intervalo de confianza para la media	Límite inferior	60,53	
		Límite superior	82,18	
	Media recortada al 5%		70,95	
	Mediana		71,00	
	Varianza		351,324	
	Desv. Desviación		18,744	
	Mínimo		50	
	Máximo		100	
	Rango		50	
	Rango intercuartil		35	
	Asimetría		,418	,597
	Curtosis		-,990	1,154
Post_test	Media		15,4286	5,29121
	95% de intervalo de confianza para la media	Límite inferior	3,9976	
		Límite superior	26,8595	
	Media recortada al 5%		14,3651	
	Mediana		,0000	
	Varianza		391,956	
	Desv. Desviación		19,79788	
	Mínimo		,00	
	Máximo		50,00	
	Rango		50,00	
	Rango intercuartil		33,00	
	Asimetría		,762	,597
	Curtosis		-1,039	1,154

TABLA XXXVIII. RESUMEN DE PRUEBA WILCOXON PARA HIPÓTESIS ESPECÍFICA 3

Resumen de prueba de hipótesis

	Hipótesis nula	Prueba	Sig.	Decisión
1	La mediana de las diferencias entre Pre_test y Post_test es igual a 0.	Prueba de rangos con signo de Wilcoxon para muestras relacionadas	,001	Rechazar la hipótesis nula.

Se muestran significaciones asintóticas. El nivel de significación es de ,05.

Si el P-valor $\geq 0{,}05$, se acepta H_0

Si el P-valor < 0,05, se acepta H_1

Paso 5: Conclusión

P-valor = 0,000 < α = 0,05

Hay una diferencia significativa en la seguridad de la información entre la prueba pre test (antes) y post test (después) de la implementación de sistema de gestión de seguridad de la información. Así se concluye el P-valor es menor a 0,05 y se acepta la H_1, es decir: El sistema de gestión de la seguridad de la información favorece significativamente el control informático de la I.E. Francisco de Zela, con un valor porcentual del 95% de confianza.

ANÁLISIS Y DISCUSIÓN DE RESULTADOS

Al haber mejorado el nivel de seguridad de información, disminuyendo las amenazas producidas y creando unas políticas de seguridad claras, se logra pasar de un promedio de75% a un 21.4% donde se evidencia una mejoría en las actualizaciones de seguridad, protección antivirus y antimalware, una división adecuada de funciones y responsabilidades, monitoreo constante de accesos no autorizados y finalmente una gestión adecuada de las contraseñas. Para [7], se mejora la seguridad de información en un 60%, al realizar una comparativa con los resultados obtenidos en nuestro caso de estudio, se mejora en un 53,6% y se llega a estar en el mismo nivel que en el antecedente.

Reducir los riesgos de información de un 67.6% a un 24.9% nos permite apreciar, que ahora se logra realizar un seguimiento de aceptación y cumplimiento de acuerdos de seguridad de la información. Para [8], un plan de tratamiento de riesgos ayuda a efectuar contramedidas a las amenazas detectadas en los activos, la reducción en nuestro caso de investigación contrasta la conclusión a la que llega el autor. También [10], menciona en sus resultados la obtención de solo un 1.3% de amenazas en rango muy alto y un 16.7% en nivel de riesgo bajo, en comparativa con nuestro caso de estudio se asemejan resultados tanto en un 16.7% para el antecedente y un 24.9% para nuestra investigación.

Al determinar la influencia de implementar un sistema de gestión de seguridad de información para los controles informáticos en la Institución Educativa “Francisco de Zela”, se observa que: el valor de significancia de la prueba Pre test es de 0,048 y luego de implementar el SGSI el valor de significancia en la prueba Post test es de 0,001. Según [11], solo el 5% del total de encuestados mencionaban que se tenía un procedimiento adecuado respecto a medidas se seguridad de la información mientras que el 95% indicaba que no se manejaban políticas respecto a este tema, por parte de esta investigación también se obtuvo datos similares donde solo el 21.7 % de los encuestados tenían una idea clara de las políticas de seguridad de información que se utilizaban en la institución y el 78,3% creía que estas políticas no están bien definidas, luego de realizar las implementaciones respectivas se logra obtener un 65% de encuestados aseverando un “nivel alto” de políticas de seguridad de la información.

CONCLUSIONES

1. Los objetivos planteados en la investigación fueron alcanzados, ya que se encontró que la aplicación del sistema de gestión de la seguridad de la información tiene un impacto notorio en la seguridad de la informática de la Institución Educativa “Francisco de Zela”.

2. Al haber mejorado el nivel de seguridad de información, disminuyendo las amenazas producidas y creando unas políticas de seguridad claras, se logra pasar de un promedio de75% a un 21.4% donde se evidencia una mejoría en las actualizaciones de seguridad, protección antivirus y antimalware, una división adecuada de funciones y responsabilidades, monitoreo constante de accesos no autorizados y finalmente una gestión adecuada de las contraseñas.

3. Reducir los riesgos de información de un 67.6% a un 24.9% nos permite apreciar, que ahora se logra realizar un seguimiento de aceptación y cumplimiento de acuerdos de seguridad de la información, el nivel de seguridad de copias de respaldo es óptimo y existe una política de escritorio limpio para evitar la divulgación de datos confidenciales.

4. Al determinar la influencia de implementar un sistema de gestión de seguridad de información para los controles informáticos en la Institución Educativa “Francisco de Zela”, se observa que: el valor de significancia de la prueba Pre test es de 0,048 y luego de implementar el SGSI el valor de significancia en la prueba Post test es de 0,001. Determinando que los datos son no paramétricos ($p<0,05$), utilizando los programas de concientización y las capacitaciones en las diversas áreas de seguridad de la información se aprecia una mejoría en el nivel de los controles informáticos.

RECOMENDACIONES

1. La Institución Educativa debe seguir mejorando y actualizando sus políticas de seguridad para asegurar que se logre cumplir con la legislación pertinente y las mejores prácticas del sector.

2. Se aconseja instalar sistemas adicionales de supervisión de la seguridad que puedan identificar y notificar a los usuarios actividades dudosas o accesos ilegales a los sistemas de datos.

3. Se recomienda aplicar la metodología de estudio para todos los activos de la Institución a fin de crear un panorama más holístico de la seguridad de la información.

4. Es recomendable aplicar una auditoría interna a fin de verificar la aceptación y cumplimiento de roles de que todos los actores de la Institución, asegurando los acuerdos de seguridad de información.

REFERENCIAS BIBLIOGRÁFICAS

[1] M. Concepción Donoso, "FORO ¿Cuán importante es la seguridad cibernética para lograr la seguridad hídrica? How important is cybersecurity to achieving water security?", *Trop J Environ Sci) e-ISSN*, vol. 56, nº 1, pp. 284–297, 2022, doi: 10.15359/rca.56-1.15.

[2] "MAPA | Mapa en tiempo real de amenazas cibernéticas Kaspersky". Accedido: 12 de diciembre de 2023. [En línea]. Disponible en: https://cybermap.kaspersky.com/es

[3] "Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021 | Blog oficial de Kaspersky". Accedido: 12 de diciembre de 2023. [En línea]. Disponible en: https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

[4] C. L. Flores, "Diseño de un sistema de gestión de seguridad de información para un instituto educativo", sep. 2013, Accedido: 1 de diciembre de 2023. [En línea]. Disponible en: https://tesis.pucp.edu.pe/repositorio//handle/20.500.12404/4721

[5] E. J. S. Chinchilla y J. S. Allende, "Riesgos de ciberseguridad en las Empresas", *Tecnología y desarrollo*, vol. 15, nº 0, dic. 2017, Accedido: 1 de diciembre de 2023. [En línea]. Disponible en: https://revistas.uax.es/index.php/tec_des/article/view/1174

[6] M. Aguilera, "¿Cuánto duran las computadoras portátiles? Guía detallada - Tecnología Android". Accedido: 3 de enero de 2024. [En línea]. Disponible en: https://tecnologiandroid.com/cuanto-duran-las-computadoras-portatiles-guia-detallada/#Vida_util_de_la_computadora_portatil_HP

[7] R. S. Zarbe Torres, "Sistema de gestión de seguridad de la información para la calidad de procesos en la I.E.P. Albert Einstein", *Universidad Nacional de Ucayali*, 2023, Accedido: 1 de diciembre de 2023. [En línea]. Disponible en: http://repositorio.unu.edu.pe/handle/UNU/6720

[8] K. L. Villadeza Romero y R. D. Condor Simon, "Diseño de un sistema de gestión de seguridad de la información basado en la norma técnica peruana -ISO/IEC 27001:2014 para la Municipalidad Distrital de Huácar 2022", 2022, Accedido: 1 de diciembre de 2023. [En línea]. Disponible en: http://repositorio.unheval.edu.pe/handle/20.500.13080/8238

[9] W. HUINCHO RAMOS, “Sistema de gestión de seguridad de la información para mejorar la protección informática de la Comisaria Región Huancavelica”, *Universidad Nacional Daniel Alcides Carrión*, oct. 2019, Accedido: 12 de diciembre de 2023. [En línea]. Disponible en: http://repositorio.undac.edu.pe/handle/undac/2017

[10] G. Hidalgo Castro, “Diseño de un sistema de gestión de seguridad de la información para la Corte Superior de Justicia de Piura, mediante la normativa ISO/IEC 27001”, *Repositorio Institucional - UCV*, 2020, Accedido: 15 de diciembre de 2023. [En línea]. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/59572

[11] J. C. Nacipucha, “Análisis y Diseño para un modelo de Gestión de la Seguridad de la Información basados en las normas ISO/IEC 27001:2013 para la empresa Artehogar en la ciudad de Guayaquil”, sep. 2019.

[12] A. Benavides Sepúlveda y C. B. Jaramillo, “Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico Model information security management system for entry-level educational institutions”, *Scientia et Technica Año XXII*, vol. 23, nº 01, 2018.

[13] E. A. Sanchez y F. L. Rebolledo, “Diseño de un Modelo de Gestión de la Seguridad de la Información en el Área de talento humano de la Secretaría de Educación”, 2017.

[14] ISO/IEC 27000:2018, “ISO/IEC 27000:2018(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary”. Accedido: 17 de diciembre de 2023. [En línea]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

[15] UNE 71504:2008, “UNE 71504:2008 Metodología de análisis y gestión de riesgos pa...” Accedido: 17 de diciembre de 2023. [En línea]. Disponible en: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0041430

[16] MAGERIT V3.0, “Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método”, 2012. [En línea]. Disponible en: http://administracionelectronica.gob.es/

[17] ISOTools Excellence, “¿Seguridad informática o seguridad de la información?” Accedido: 18 de diciembre de 2023. [En línea]. Disponible en: https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

[18] J. A. Figueroa-Suárez, R. F. Rodríguez-Andrade, C. C. Bone-Obando, y J. A. Saltos-Gómez, "La seguridad informática y la seguridad de la información", *Polo del Conocimiento*, vol. 2, nº 12, p. 145, mar. 2018, doi: 10.23857/pc.v2i12.420.

[19] R. K. Moron, "Diseño e implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú S.A.C", *Repositorio Institucional - USS*, 2023, Accedido: 18 de diciembre de 2023. [En línea]. Disponible en: http://repositorio.uss.edu.pe//handle/20.500.12802/10629

[20] R. Hernández Sampieri, "Metodología de la investigación".

[21] Hispanic Net.org, "Consideraciones éticas en la investigación | Tipos y ejemplos | Hispanic Net". Accedido: 21 de diciembre de 2023. [En línea]. Disponible en: https://hispanic-net.org/una-gu%C3%ADa-de-consideraciones-%C3%A9ticas-en-la-investigaci%C3%B3n/

[22] IE Francisco de Zela, "Reglamento Interno 'Francisco de Zela'", Huancayo, mar. 2023.

[23] "Ley N.° 28044 - Normas y documentos legales - Congreso de la República - Plataforma del Estado Peruano". Accedido: 25 de marzo de 2024. [En línea]. Disponible en: https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/118378-28044

ANEXOS

Anexo 01. Matriz de Consistencia

TABLA XXXIX. MATRIZ DE CONSISTENCIA

PROBLEMA	OBJETIVO	HIPÓTESIS	METODOLOGÍA	POBLACIÓN
Problema General: ¿En qué medida el sistema de gestión de la seguridad de la información favorece la seguridad informática de la I.E. Francisco de Zela?	**Objetivo General:** Determinar en qué medida el sistema de gestión de la seguridad de la información favorece la seguridad informática de la I.E. Francisco de Zela.	**Hipótesis General:** El sistema de gestión de la seguridad de la información favorece significativamente la seguridad informática de la I.E. Francisco de Zela.	El tipo de investigación utilizado en nuestra investigación es de tipo aplicada. Dentro de este marco utilizaremos la ISO/IEC 27001. **Nivel:** Descriptiva **Diseño:** Pre experimental con dos grupos no equivalentes, con pre test y post test. GE: 0_1 X 0_2 GC: 0_3 0_4 Donde: G.E. Grupo Experimental. G.C. Grupo de Control. 0_1 y 0_3 Pre Test 0_2 y 0_4 Post Test X: Manipulación de la Variable dependiente.	**Población:** Los datos de los 271 actores de la comunidad educativa. **Muestra:** Para fines de esta investigación se tomarán los mismos datos de la población y considerando el personal que labora en la institución, haciendo un total de: 29 personas. **Técnicas e instrumentos** Encuesta: cuestionario de encuesta Fichas de observación. **Técnicas de procesamiento de datos** Estadística descriptiva Tablas de frecuencia
Problemas específicos: • ¿En qué medida el sistema de gestión de la seguridad de la información favorece la seguridad de la información de la I.E. Francisco de Zela? • ¿En qué medida el sistema de gestión de la seguridad de la información favorece la gestión de riesgos de la información de la I.E. Francisco de Zela? • ¿En qué medida el sistema de gestión de la seguridad de la información favorece el control informático de la I.E. Francisco de Zela?	**Objetivos Específicos:** • Determinar en qué medida el sistema de gestión de la seguridad de la información favorece la seguridad de información de la I.E. Francisco de Zela. • Determinar en qué medida el sistema de gestión de la seguridad de la información favorece la gestión de riesgos de la información de la I.E. Francisco de Zela. • Determinar en qué medida el sistema de gestión de la seguridad de la información favorece el control informático de la I.E. Francisco de Zela.	**Hipótesis Específicas:** • El sistema de gestión de la seguridad de la información favorece significativamente la seguridad de información de la I.E. Francisco de Zela • El sistema de gestión de la seguridad de la información favorece significativamente la gestión de riesgos de la información de la I.E. Francisco de Zela • El sistema de gestión de la seguridad de la información favorece significativamente el control informático de la I.E. Francisco de Zela		

Anexo 02. Matriz de Operacionalización de las Variables

TABLA XL. MATRIZ DE OPERACIONALIZACIÓN DE LAS VARIABLES

Variables	Definición Conceptual	Dimensiones	Indicadores	Ítems	Formula	Instrumento
Variable Independiente: Sistema de Gestión de la Seguridad de la Información	"Los elementos interrelacionados o que interactúan (estructura organizacional, políticas, planes de acción, responsabilidades, procesos, un conjunto de procedimientos y recursos). Basados en la Gestión de riesgos y mejora continua"[14].	Diagnóstico de situación actual	Activos identificados y valorados	Cantidad de activos	% de frecuencia con que se repite	Guía de Observación 1
			Amenazas sobre activos de información	Cantidad de amenazas	% de frecuencia con que se repite	Guía de Observación 2
			Vulnerabilidades sobre activos de información	Cantidad de vulnerabilidades	% de frecuencia con que se repite	Guía de Observación 3
			Estimación del nivel de riesgo	Riesgo bajo, medio, alto	% del total	Guía de Observación 4
		Implementación del SGSI	Controles aplicados según normativa	Políticas de seguridad de información, Seguridad de recursos humanos	Porcentaje de cumplimiento	Lista de control 1
			Tasa de incidencias registradas	Tasa de incidencias registradas	Cantidad de incidencias	Guía de observación 5
		Monitoreo y revisión	Indicadores para procedimientos de monitorización	Nivel de conocimiento de la política de seguridad en colaboradores	Frecuencia de medición semestral	Lista de control 2
Variable dependiente: Seguridad Informática	"La seguridad informática busca proteger los sistemas informáticos y garantizar la integridad y confidencialidad de la información que contienen"[17].	Seguridad de la Información	Nivel de seguridad de equipos	¿El nivel de actualizaciones de seguridad, soluciones antivirus y antimalware son óptimos para trabajar en la institución?	$SI = \frac{R}{T} X100$ Donde: SI: Seguridad de información T: Total de encuestados R: Respuestas	Cuestionario Encuesta Ficha de observación
			Nivel de políticas de gestión de contraseñas	¿Se almacena y gestiona las contraseñas de forma segura?		
			Nivel de políticas de control de acceso	¿Se registran y monitorean intentos de acceso no autorizados?		
			Nivel de segregación de funciones y responsabilidades	¿En qué nivel se encuentran dividas las funciones y responsabilidades a fin de reducir los cambios sin autorización o el uso indebido de información o servicios?		
			Nivel de aseguramiento de controles de seguridad	¿Se tienen políticas de acceso físico y procedimientos establecidos para la gestión de incidentes de seguridad?		
			Nivel de procedimientos para eliminación de accesos	¿En qué escala, existe un procedimiento para garantizar que al término del vínculo laboral los usuarios sean deshabilitados de todos los accesos informáticos?		

		Riesgo de la información	Nivel de aceptación de acuerdos	¿Se realiza un seguimiento de la aceptación y cumplimiento del acuerdo de seguridad por parte de los usuarios?	$RDI = \frac{RRDI}{TRDI} x100$ Donde: RDI: Riesgo de la Información RRDI: Respuestas TRDI: Total de encuestados	
			Nivel de existencia de procedimientos de destrucción	¿Existe un procedimiento para destruir los datos obsoletos o inútiles?		
			Nivel de protección de datos	¿El nivel de seguridad de las copias de respaldo son los óptimos para proteger los datos y documentos contra, destrucción, perdida, falsificación, accesos y divulgación no autorizada?		
			Nivel de planes para la continuidad operativa	¿Se maneja una política de escritorio limpio a fin de evitar divulgación de datos confidenciales?		
		Control informático	Nivel de capacitaciones de seguridad de la información	¿Se proporciona capacitaciones en seguridad de la información a todos los usuarios de los equipos informáticos de la Institución?	$IC = \frac{TIC}{TICD} x100$ Donde: IC: Control informático TIC: Respuestas TCID: Total de encuestados	
			Nivel de concientización de la seguridad de información	¿Se elabora un plan de concientización respecto a temas de seguridad de la información?		

Anexo 03. Matriz de Operacionalización del Instrumento

TABLA XLI OPERALIZACIÓN DEL INSTRUMENTO

Variable	Dimensión	Indicador	Ítem	Escala de Medición	Instrumento
Variable dependiente: Seguridad Informática	Seguridad de la Información	Nivel de seguridad de equipos	¿El nivel de actualizaciones de seguridad, soluciones antivirus y antimalware son óptimos para trabajar en la institución?	Alto= 2, Medio= 1, Nulo = 0	Encuesta
		Nivel de políticas de gestión de contraseñas	¿Se almacena y gestiona las contraseñas de forma segura?	Alto= 2, Medio= 1, Nulo = 0	
		Nivel de políticas de control de acceso	¿Se registran y monitorean intentos de acceso no autorizados?	Alto= 2, Medio= 1, Nulo = 0	
		Nivel de segregación de funciones y responsabilidades	¿En qué nivel se encuentran dividas las funciones y responsabilidades a fin de reducir los cambios sin autorización o el uso indebido de información o servicios?	Alto= 2, Medio= 1, Nulo = 0	
		Nivel de aseguramiento de controles de seguridad	¿Se tienen políticas de acceso físico y procedimientos establecidos para la gestión de incidentes de seguridad?	Alto= 2, Medio= 1, Nulo = 0	
		Nivel de procedimientos para deshabilitar accesos	¿En qué escala, existe un procedimiento para garantizar que al término del vínculo laboral los usuarios sean deshabilitados de todos los accesos informáticos?	Alto= 2, Medio= 1, Nulo = 0	
	Riesgo de la información	Nivel de aceptación de acuerdos	¿Se realiza un seguimiento de la aceptación y cumplimiento del acuerdo de seguridad por parte de los usuarios?	Alto= 2, Medio= 1, Nulo = 0	
		Nivel de existencia de procedimientos de destrucción	¿Existe un procedimiento para destruir los datos obsoletos o inútiles?	Alto= 2, Medio= 1, Nulo = 0	
		Nivel de protección de datos	¿El nivel de seguridad de las copias de respaldo son los óptimos para proteger los datos y documentos contra, destrucción, perdida, falsificación, accesos y divulgación no autorizada?	Alto= 2, Medio= 1, Nulo = 0	
		Nivel de filtración de la privacidad	¿Se maneja una política de escritorio limpio a fin de evitar divulgación de datos confidenciales?	Alto= 2, Medio= 1, Nulo = 0	
	Control informático	Nivel de capacitaciones de seguridad de la información	¿Se proporciona capacitaciones en seguridad de la información a todos los usuarios de los equipos informáticos de la Institución?	Alto= 2, Medio= 1, Nulo = 0	
		Nivel de concientización de la seguridad de información	¿Se elabora un plan de concientización respecto a temas de seguridad de la información?	Alto= 2, Medio= 1, Nulo = 0	

Anexo 04. Instrumento de Investigación

a. Ficha de registro Pre Test para seguridad de la información

TABLA XLII. FICHA DE REGISTRO PRE TEST PARA SEGURIDAD DE LA INFORMACIÓN

<table>
<tr><td>Investigador:</td><td colspan="4"></td></tr>
<tr><td>Institución educativa:</td><td colspan="4"></td></tr>
<tr><td>Dirección:</td><td colspan="4"></td></tr>
<tr><td>Fecha de inicio:</td><td colspan="4"></td></tr>
<tr><td>Fecha de terminación:</td><td colspan="4"></td></tr>
<tr><td>Variable:</td><td colspan="4">Formula:</td></tr>
<tr><td colspan="2">Reportes:</td><td colspan="3" rowspan="3">$SI = \frac{RAS}{TAS} X100$
Donde:
SI: Seguridad de información
TAS: Total de accesos de seguridad de información
RAS: Reporte de accesos solucionados al día</td></tr>
<tr><td>Indicador</td><td>Medida</td></tr>
<tr><td>Seguridad de la información (pre test)</td><td>Porcentaje</td></tr>
<tr><td>Ítem</td><td>Fecha</td><td>RAS</td><td>TAS</td><td>SI</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>TOTAL</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="3">PROMEDIO</td><td></td></tr>
</table>

b. Ficha de registro Post test para seguridad de la información

TABLA XLIII. FICHA DE REGISTRO POST TEST PARA SEGURIDAD DE INFORMACIÓN

<table>
<tr><td>Investigador:</td><td colspan="4"></td></tr>
<tr><td>Institución educativa:</td><td colspan="4"></td></tr>
<tr><td>Dirección:</td><td colspan="4"></td></tr>
<tr><td>Fecha de inicio:</td><td colspan="4"></td></tr>
<tr><td>Fecha de terminación:</td><td colspan="4"></td></tr>
<tr><td>Variable:</td><td colspan="4">Formula:</td></tr>
<tr><td colspan="2">Reportes:</td><td colspan="3" rowspan="3">$SI = \frac{RAS}{TAS} X100$
Donde:
SI: Seguridad de información
TAS: Total de accesos de seguridad de información
RAS: Reporte de accesos solucionados al día</td></tr>
<tr><td>Indicador</td><td>Medida</td></tr>
<tr><td>Seguridad de la información (post test)</td><td>Porcentaje</td></tr>
<tr><td>Ítem</td><td>Fecha</td><td>RAS</td><td>TAS</td><td>SI</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>TOTAL</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="3">PROMEDIO</td><td></td></tr>
</table>

c. Ficha de registro Pre Test para riesgo informático

TABLA XLIV. FICHA DE REGISTRO PRE TEST PARA RIESGO INFORMÁTICO

<table>
<tr><td>Investigador:</td><td colspan="4"></td></tr>
<tr><td>Institución educativa:</td><td colspan="4"></td></tr>
<tr><td>Dirección:</td><td colspan="4"></td></tr>
<tr><td>Fecha de inicio:</td><td colspan="4"></td></tr>
<tr><td>Fecha de terminación:</td><td colspan="4"></td></tr>
<tr><td>Variable:</td><td colspan="4">Formula:</td></tr>
<tr><td colspan="2">Reportes:</td><td colspan="3" rowspan="4">$RDI = \frac{RRDI}{TRDI} x100$
Donde:
RDI: Riesgo de la Información
RRDI: Reporte de riesgos de información solucionados al día
TRDI: Total de riesgo de la información al día</td></tr>
<tr><td>Indicador</td><td>Medida</td></tr>
<tr><td></td><td></td></tr>
<tr><td>Riesgo informático (pre test)</td><td>Porcentaje</td></tr>
<tr><td>Ítem</td><td>Fecha</td><td>RRDI</td><td>TRDI</td><td>RDI%</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>TOTAL</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="3">PROMEDIO</td><td></td></tr>
</table>

d. Ficha de registro Post test para riesgo informático

TABLA XLV. FICHA DE REGISTRO POST TEST PARA RIESGO INFORMÁTICO

<table>
<tr><td>Investigador:</td><td colspan="4"></td></tr>
<tr><td>Institución educativa:</td><td colspan="4"></td></tr>
<tr><td>Dirección:</td><td colspan="4"></td></tr>
<tr><td>Fecha de inicio:</td><td colspan="4"></td></tr>
<tr><td>Fecha de terminación:</td><td colspan="4"></td></tr>
<tr><td>Variable:</td><td colspan="4">Formula:</td></tr>
<tr><td colspan="2">Reportes:</td><td colspan="3" rowspan="4">$RDI = \frac{RRDI}{TRDI} x100$
Donde:
RDI: Riesgo de la Información
RRDI: Reporte de riesgos de información solucionados al día
TRDI: Total de riesgo de la información al día</td></tr>
<tr><td>Indicador</td><td>Medida</td></tr>
<tr><td>Riesgo informático acción (post test)</td><td>Porcentaje</td></tr>
<tr><td>Ítem</td><td>Fecha</td><td>RRDI</td><td>TRDI</td><td>RDI%</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>TOTAL</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="3">PROMEDIO</td><td></td></tr>
</table>

e. Ficha de registro Pre Test para control informático

TABLA XLVI. FICHA DE REGISTRO PRE TEST PARA CONTROL INFORMÁTICO

<table>
<tr><td>Investigador:</td><td colspan="4"></td></tr>
<tr><td>Institución educativa:</td><td colspan="4"></td></tr>
<tr><td>Dirección:</td><td colspan="4"></td></tr>
<tr><td>Fecha de inicio:</td><td colspan="4"></td></tr>
<tr><td>Fecha de terminación:</td><td colspan="4"></td></tr>
<tr><td>Variable:</td><td colspan="4">Formula:</td></tr>
<tr><td colspan="2">Reportes:</td><td colspan="3" rowspan="3">$IC = \frac{TIC}{TICD} x100$
Donde:
IC: Control informático
TIC: Total controles informáticos
TCID: Total de controles aplicados al día</td></tr>
<tr><td>Indicador</td><td>Medida</td></tr>
<tr><td>Control informático (pre test)</td><td>Porcentaje</td></tr>
<tr><td>Ítem</td><td>Fecha</td><td>TIC</td><td>TCID</td><td>IC%</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>TOTAL</td><td></td><td></td><td></td></tr>
<tr><td></td><td>PROMEDIO</td><td colspan="3"></td></tr>
</table>

f. Ficha de registro Post test para control informático

TABLA XLVII. FICHA DE REGISTRO POST TEST PARA CONTROL INFORMÁTICO

<table>
<tr><td>Investigador:</td><td colspan="4"></td></tr>
<tr><td>Institución educativa:</td><td colspan="4"></td></tr>
<tr><td>Dirección:</td><td colspan="4"></td></tr>
<tr><td>Fecha de inicio:</td><td colspan="4"></td></tr>
<tr><td>Fecha de terminación:</td><td colspan="4"></td></tr>
<tr><td>Variable:</td><td colspan="4">Formula:</td></tr>
<tr><td colspan="2">Reportes:</td><td colspan="3" rowspan="3">$IC = \frac{TIC}{TICD} x100$
Donde:
IC: Control informático
TIC: Total controles informáticos
TCID: Total de controles aplicados al día</td></tr>
<tr><td>Indicador</td><td>Medida</td></tr>
<tr><td>Control informático (post test)</td><td>Porcentaje</td></tr>
<tr><td>Ítem</td><td>Fecha</td><td>TIC</td><td>TCID</td><td>IC%</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>TOTAL</td><td></td><td></td><td></td></tr>
<tr><td></td><td>PROMEDIO</td><td colspan="3"></td></tr>
</table>

UNIVERSIDAD PERUANA LOS ANDES

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

ENCUESTA

Instrucciones: Lea atentamente cada pregunta y responda marcando el número según criterio. La encuesta es totalmente anónima y tiene como objetivo garantizar que usted sea lo más veraz y honesto posible.

Criterios:

Alto = 2
Medio = 1
Nulo = 0

Ítems	Respuesta	Observaciones
1. ¿El nivel de actualizaciones de seguridad, soluciones antivirus y antimalware son óptimos para trabajar en la institución?		
2. ¿Se almacena y gestiona las contraseñas de forma segura?		
3. ¿Se registran y monitorean intentos de acceso no autorizados?		
4. ¿En qué nivel se encuentran dividas las funciones y responsabilidades a fin de reducir los cambios sin autorización o el uso indebido de información o servicios?		
5. ¿Se tienen políticas de acceso físico y procedimientos establecidos para la gestión de incidentes de seguridad?		
6. ¿En qué escala, existe un procedimiento para garantizar que al término del vínculo laboral los usuarios sean deshabilitados de todos los accesos informáticos?		
7. ¿Se realiza un seguimiento de la aceptación y cumplimiento del acuerdo de seguridad por parte de los usuarios?		
8. ¿Existe un procedimiento para destruir los datos obsoletos o inútiles?		
9. ¿El nivel de seguridad de las copias de respaldo son los óptimos para proteger los datos y documentos contra, destrucción, perdida, falsificación, accesos y divulgación no autorizada?		
10. ¿Se maneja una política de escritorio limpio a fin de evitar divulgación de datos confidenciales?		
11. ¿Se proporciona capacitaciones en seguridad de la información a todos los usuarios de los equipos informáticos de la Institución?		
12. ¿Se elabora un plan de concientización respecto a temas de seguridad de la información?		

Anexo 05 Confiabilidad y validez del instrumento

Ficha de Evaluación de Experto 1

FICHA DE EVALUACIÓN DE EXPERTOS

La presente ficha forma parte de la investigación **"Sistema de gestión de la seguridad de la información para mejorar la seguridad informática de la I.E. Francisco de Zela – Huancayo - 2024".**

DATOS DEL EXPERTO:

Nombres y Apellidos: Magno Baldeón Tovar	DNI N°: 19427794
Título Profesional: Ingeniero de Sistemas.	
Grado Académico: Dr. Administración de la Educación	
Mención:	
Institución donde trabaja: Universidad Peruana Los Andes	

ESCALA DICOTÓMICA PARA EVALUAR NIVEL DE VALIDEZ DEL INSTRUMENTO

Nota: Marque con un aspa "X" dentro del recuadro de valoración, que usted considere pertinente.

N°	CRITERIOS	SI	NO
1	El instrumento tiene estructura lógica	✓	
2	La secuencia de presentación es optima	✓	
3	El grado de dificultad o complejidad de los ítems es aceptable		✓
4	Los términos utilizados en las preguntas son claros y comprensibles	✓	
5	Los reactivos reflejan el problema de investigación	✓	
6	El instrumento abarca en su totalidad el problema de investigación	✓	
7	Los ítems permiten medir el problema de investigación	✓	
8	Los ítems permiten recoger información para alcanzar los objetivos de la investigación	✓	
9	El instrumento abarca las variables e indicadores	✓	
10	Los ítems permiten contrastar la hipótesis	✓	

SUGERENCIAS:

Firma

Ficha de Evaluación de Experto 2

FICHA DE EVALUACIÓN DE EXPERTOS

La presente ficha forma parte de la investigación **"Sistema de gestión de la seguridad de la información para mejorar la seguridad informática de la I.E. Francisco de Zela – Huancayo - 2024".**

DATOS DEL EXPERTO:

Nombres y Apellidos: Edward Bustinza Zuasnábar	DNI N°: 20111231
Título Profesional: Ingeniero de Sistemas	
Grado Académico: Dr. Ingeniería de Sistemas	
Mención: Doctor en Sistemas de Ingeniería	
Institución donde trabaja: UNIVERSIDAD PERUANA LOS ANDES	

ESCALA DICOTÓMICA PARA EVALUAR NIVEL DE VALIDEZ DEL INSTRUMENTO

Nota: Marque con un aspa "X" dentro del recuadro de valoración, que usted considere pertinente.

N°	CRITERIOS	SI	NO
1	El instrumento tiene estructura lógica	✓	
2	La secuencia de presentación es optima	✓	
3	El grado de dificultad o complejidad de los ítems es aceptable	✓	
4	Los términos utilizados en las preguntas son claros y comprensibles	✓	
5	Los reactivos reflejan el problema de investigación	✓	
6	El instrumento abarca en su totalidad el problema de investigación	✓	
7	Los ítems permiten medir el problema de investigación	✓	
8	Los ítems permiten recoger información para alcanzar los objetivos de la investigación		✓
9	El instrumento abarca las variables e indicadores	✓	
10	Los ítems permiten contrastar la hipótesis	✓	

SUGERENCIAS:

Firma del Experto

Dr. Edward Eddie Bustinza Zuasnábar
INGENIERO DE SISTEMA
REG. CIP. N° 87669

Ficha de Evaluación de Experto 3

FICHA DE EVALUACIÓN DE EXPERTOS

La presente ficha forma parte de la investigación **"Sistema de gestión de la seguridad de la información para mejorar la seguridad informática de la I.E. Francisco de Zela – Huancayo - 2024".**

ESCALA DICOTÓMICA PARA EVALUAR NIVEL DE VALIDEZ DEL INSTRUMENTO

Nota: Marque con un aspa "X" dentro del recuadro de valoración, que usted considere pertinente.

N°	CRITERIOS	SI	NO
1	El instrumento tiene estructura lógica	X	
2	La secuencia de presentación es optima	X	
3	El grado de dificultad o complejidad de los ítems es aceptable	X	
4	Los términos utilizados en las preguntas son claros y comprensibles	X	
5	Los reactivos reflejan el problema de investigación	X	
6	El instrumento abarca en su totalidad el problema de investigación	X	
7	Los ítems permiten medir el problema de investigación	X	
8	Los ítems permiten recoger información para alcanzar los objetivos de la investigación	X	
9	El instrumento abarca las variables e indicadores	X	
10	Los ítems permiten contrastar la hipótesis	X	

SUGERENCIAS:

DATOS DEL EXPERTO:

Nombres y Apellidos	ALFREDO H. YAPIAS ROJAS	DNI N°	21289235
Título Profesional	INGENIERO DE SISTEMAS Y COMPUTACION		
Grado Académico	MAGISTER		
Mención	DIDACTICA Y TECNOLOGIAS DE LA INFORMACION Y C.		
Institución donde trabaja	UNIVERSIDAD PERUANA LOS ANDES		

Mg. Alfredo H. Yapias Rojas
CIP 111371
Firma

Anexo 06 Base de datos recolectados y evidencia de su procesamiento

Fecha	Activo	Ubicación	Incidencia	Resuelto	Satisfacción del usuario	tipo de acción
27/11/2023	Laptop	Aula de Innovación	Acceso no autorizado a utilizar laptop del aula	NO	Insatisfecho	seguridad información
27/11/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°4	NO	Neutral	riesgo informático
27/11/2023	Laptop	Aula 01	Troyano encontrado en la laptop N°41	SI	Neutral	riesgo informático
27/11/2023	Laptop	Aula 01	Troyano encontrado en la laptop N°48	SI	Neutral	riesgo informático
27/11/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°23	NO	Neutral	riesgo informático
27/11/2023	Laptop	Aula de Innovación	No se encuentra UPS para protección de equipos	NO	Insatisfecho	riesgo informático
27/11/2023	Laptop	Aula 01	No se encuentra UPS para protección de equipos	SI	Insatisfecho	riesgo informático
27/11/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°32	NO	Insatisfecho	riesgo informático
27/11/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°24	NO	Insatisfecho	riesgo informático
27/11/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°15	NO	Insatisfecho	riesgo informático
27/11/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°28	NO	Insatisfecho	riesgo informático
27/11/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°23	NO	Insatisfecho	riesgo informático
27/11/2023	Equipo de sonido	Aula de Innovación	Utilización del equipo sin autorización	NO	Insatisfecho	seguridad información
27/11/2023	Amplificador de audio	Almacén	Utilización del equipo sin autorización	SI	Satisfecho	seguridad información
28/11/2023	PC	Dirección	Acceso no autorizado a utilizar PC de la dirección	SI	Insatisfecho	seguridad información
28/11/2023	Laptop	Aula de Innovación	Infección de virus por usb	SI	Satisfecho	control informático
28/11/2023	PC	Almacén	no se encuentra registro del equipo	NO	Insatisfecho	control informático
28/11/2023	Laptop	Aula de Innovación	Infección de virus por usb	SI	Insatisfecho	control informático

28/11/2023	Laptop	Aula de Innovación	Infección de virus por usb	NO	Insatisfecho	control informático
28/11/2023	Laptop	Aula de Innovación	Actualización de software desfasada	NO	Insatisfecho	control informático
28/11/2023	Laptop	Aula de Innovación	Acceso no autorizado a utilizar laptop del aula	NO	Neutral	seguridad información
29/11/2023	Laptop	Aula de Innovación	Instalación de programas no autorizados laptop 14	NO	Insatisfecho	control informático
29/11/2023	Laptop	Aula de Innovación	Instalación de programas no autorizados laptop 10	NO	Insatisfecho	control informático
29/11/2023	Laptop	Aula de Innovación	Instalación de programas no autorizados laptop 25	SI	Satisfecho	control informático
30/11/2023	Laptop	Aula de Innovación	Instalación de programas no autorizados laptop 12	NO	Insatisfecho	control informático
29/11/2023	Laptop	Aula 05	Troyano encontrado en la laptop N°87	NO	Insatisfecho	riesgo informático
29/11/2023	Laptop	Aula 08	Troyano encontrado en la laptop N°83	NO	Insatisfecho	riesgo informático
29/11/2023	Laptop	Aula 10	Troyano encontrado en la laptop N°82	NO	Insatisfecho	riesgo informático
29/11/2023	Laptop	Aula 01	Troyano encontrado en la laptop N°53	SI	Satisfecho	riesgo informático
29/11/2023	Laptop	Aula 04	Troyano encontrado en la laptop N°88	NO	Insatisfecho	riesgo informático
29/11/2023	Reg. Asistencia estudiantes	Caseta auxiliar	Perdida del registro de asistencia de estudiantes	NO	Completamente Insatisfecho	seguridad información
29/11/2023	Ficha de monitoreo	Coord. Ciencias	Daño físico en la ficha de monitoreo	NO	Insatisfecho	seguridad información
29/11/2023	Laptop	Aula de Innovación	Acceso no autorizado a utilizar laptop del aula	NO	Insatisfecho	seguridad información
29/11/2023	Laptop	Aula de Innovación	Acceso no autorizado a utilizar laptop del aula	SI	Neutral	seguridad información
29/11/2023	Laptop	Aula de Innovación	Error en configuración de la laptop N°08	SI	Satisfecho	riesgo informático
30/11/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°12	SI	Neutral	riesgo informático
30/11/2023	Televisor	Aula 05	Utilización del equipo sin autorización	NO	Insatisfecho	seguridad información
30/11/2023	Reg. Asistencia trabajadores	Dirección	Registro de asistencia marcado fuera de la hora	NO	Insatisfecho	seguridad información
30/11/2023	Fotocopiadora	Dirección	Utilización del equipo sin autorización	SI	Neutral	seguridad información
30/11/2023	Laptop	Aula 08	Utilización del equipo sin autorización	NO	Insatisfecho	seguridad información

30/11/2023	Impresora	Dirección	Utilización del equipo sin autorización	NO	Insatisfecho	seguridad información
1/12/2023	Laptop	Aula de Innovación	Acceso no autorizado a utilizar laptop del aula	SI	Satisfecho	seguridad información
1/12/2023	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Satisfecho	riesgo informático
1/12/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°31	NO	Insatisfecho	riesgo informático
1/12/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°14	NO	Insatisfecho	riesgo informático
1/12/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°08	NO	Insatisfecho	riesgo informático
1/12/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°02	NO	Insatisfecho	riesgo informático
1/12/2023	Estabilizador	Aula de Innovación	Daño físico en el estabilizador por causa de descargas eléctricas	NO	Insatisfecho	riesgo informático
1/12/2023	Disco duro externo	Aula de Innovación	Perdida de información sobre software educativo	NO	Satisfecho	seguridad información
1/12/2023	Laptop	Aula 01	Acceso no autorizado a utilizar laptop del aula	NO	Insatisfecho	seguridad información
1/12/2023	Impresora	Dirección	Obstrucción de papel en la impresora	SI	Satisfecho	riesgo informático
4/12/2023	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Insatisfecho	riesgo informático
4/12/2023	Laptop	Aula 01	Troyano encontrado en la laptop N°57	NO	Insatisfecho	riesgo informático
4/12/2023	Laptop	Aula 01	Troyano encontrado en la laptop N°65	NO	Insatisfecho	riesgo informático
4/12/2023	Proyector	Aula 08	Error en configuración del proyector	NO	Insatisfecho	control informático
4/12/2023	Laptop	Aula 01	Troyano encontrado en la laptop N°62	NO	Insatisfecho	riesgo informático
4/12/2023	Proyector	Aula 10	Error en configuración del proyector	NO	Insatisfecho	control informático
4/12/2023	Proyector	Aula 06	Error en configuración del proyector	SI	Satisfecho	control informático
5/12/2023	Laptop	Aula 01	Troyano encontrado en la laptop N°42	SI	Insatisfecho	riesgo informático
5/12/2023	Proyector	Aula 07	Utilización del equipo sin autorización	NO	Insatisfecho	seguridad información
5/12/2023	Fotocopiadora	Dirección	Utilización del equipo sin autorización	SI	Satisfecho	seguridad información
5/12/2023	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Insatisfecho	riesgo informático
5/12/2023	Laptop	Aula de Innovación	Acceso no autorizado a utilizar laptop del aula	NO	Insatisfecho	seguridad información
6/12/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°30	NO	Insatisfecho	riesgo informático

6/12/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°17	NO	Insatisfecho	riesgo informático
6/12/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°18	NO	Insatisfecho	riesgo informático
6/12/2023	Laptop	Aula 10	Acceso no autorizado a utilizar laptop del aula	NO	Insatisfecho	seguridad información
6/12/2023	Laptop	Aula 05	Acceso no autorizado a utilizar laptop del aula	NO	Insatisfecho	seguridad información
6/12/2023	Laptop	Aula 01	Actualización de software desfasada	SI	Neutral	control informático
7/12/2023	Proyector	Aula 09	Utilización del equipo sin autorización	NO	Insatisfecho	seguridad información
7/12/2023	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Satisfecho	riesgo informático
7/12/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°13	NO	Insatisfecho	riesgo informático
7/12/2023	Proyector	Aula 03	Utilización del equipo sin autorización	NO	Insatisfecho	seguridad información
7/12/2023	Proyector	Aula 05	Utilización del equipo sin autorización	NO	Insatisfecho	seguridad información
7/12/2023	Proyector	Aula 10	Utilización del equipo sin autorización	NO	Insatisfecho	seguridad información
7/12/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°17	NO	Insatisfecho	riesgo informático
7/12/2023	Ficha de monitoreo	Coord. Tutotía	Daño físico en la ficha de monitoreo	SI	Satisfecho	seguridad información
7/12/2023	Office	Coord. Letras	Error en activación del producto	NO	Insatisfecho	control informático
7/12/2023	Office	Coord. Ciencias	Error en activación del producto	NO	Insatisfecho	control informático
7/12/2023	Office	Coord. Tutotía	Error en activación del producto	NO	Insatisfecho	control informático
8/12/2023	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Insatisfecho	riesgo informático
8/12/2023	Cámara de vigilancia	Dirección	Falla en la cámara de seguridad	NO	Insatisfecho	riesgo informático
8/12/2023	Proyector	Aula 06	Error en configuración del proyector	SI	Satisfecho	control informático
11/12/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°26	SI	Insatisfecho	riesgo informático
11/12/2023	Office	Caseta auxiliar	Error en activación del producto en laptop prestada a la auxiliar	SI	Satisfecho	control informático
11/12/2023	Contraseñas	Aula de Innovación	Inicio de sesión no autorizada en laptop N°35	NO	Insatisfecho	seguridad información
11/12/2023	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Insatisfecho	riesgo informático
11/12/2023	Contraseñas	Aula de Innovación	Inicio de sesión no autorizada en laptop N°39	NO	Insatisfecho	seguridad información

12/12/2023	Sistema operativo	Aula 01	Error en la activación del producto en laptop N°49	NO	Insatisfecho	control informático
12/12/2023	Sistema operativo	Aula 01	Error en la activación del producto en laptop N°56	NO	Insatisfecho	control informático
12/12/2023	Sistema operativo	Aula 01	Error en la activación del producto en laptop N°59	NO	Insatisfecho	control informático
12/12/2023	Sistema operativo	Aula 01	Error en la activación del producto en laptop N°61	NO	Insatisfecho	control informático
12/12/2023	Laptop	Aula 01	Troyano encontrado en la laptop N°52	SI	Satisfecho	riesgo informático
12/12/2023	Laptop	Aula 01	Troyano encontrado en la laptop N°55	NO	Insatisfecho	riesgo informático
12/12/2023	Laptop	Aula 01	Troyano encontrado en la laptop N°42	NO	Insatisfecho	riesgo informático
12/12/2023	Office	Aula de Innovación	Error en activación del producto en laptop N°12	NO	Insatisfecho	control informático
13/12/2023	Fotocopiadora	Dirección	Acceso no autorizado	NO	Insatisfecho	seguridad información
13/12/2023	Equipo de sonido	Almacén	Acceso no autorizado	NO	Insatisfecho	seguridad información
13/12/2023	Impresora	Dirección	Acceso no autorizado	SI	Insatisfecho	seguridad información
13/12/2023	Laptop	Aula 10	Laptop no prpyecta imagen en el proyector	SI	Neutral	control informático
13/12/2023	Televisor	Aula 07	Televisor no tiene manual de uso para configurar uso del proyector	NO	Insatisfecho	control informático
13/12/2023	Laptop	Aula 01	Troyano encontrado en la laptop N°59	SI	Insatisfecho	riesgo informático
14/12/2023	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Insatisfecho	riesgo informático
14/12/2023	Laptop	Aula 08	Laptop no proyecta imagen en el proyector	NO	Neutral	riesgo informático
15/12/2023	Proyector	Aula 03	Acceso no autorizado	SI	Insatisfecho	seguridad información
15/12/2023	Impresora	Dirección	Acceso no autorizado	NO	Insatisfecho	seguridad información
15/12/2023	Impresora	Aula 01	Acceso no autorizado	NO	Insatisfecho	seguridad información
15/12/2023	Proyector	Aula 06	Error en configuración del proyector	SI	Satisfecho	control informático
15/12/2023	Equipo de sonido	Almacén	Equipo de sonido poco usado fue probado y dejó de funcionar	NO	Insatisfecho	riesgo informático
15/12/2023	Office	Dirección	Error en activación del producto	NO	Insatisfecho	control informático
19/12/2023	Laptop	Aula 01	Troyano encontrado en la laptop N°68	SI	Satisfecho	riesgo informático
19/12/2023	Reg. Asistencia trabajadores	Dirección	Quejas por falta de control en ingreso del personal	NO	Insatisfecho	seguridad información
19/12/2023	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Insatisfecho	riesgo informático
19/12/2023	Sistema operativo	Aula 01	Error en la activación del producto en laptop N°62	NO	Insatisfecho	control informático
19/12/2023	Memorandums	Aula de Innovación	Pérdida de memorandums N°24, N°26 y N°27	NO	Insatisfecho	seguridad información

19/12/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°18	SI	Insatisfecho	riesgo informático
19/12/2023	Proyector	Aula 09	Error en configuración del proyector	SI	Satisfecho	control informático
20/12/2023	Laptop	Aula de Innovación	Acceso no autorizado a utilizar laptop del aula	NO	Insatisfecho	seguridad información
20/12/2023	Laptop	Aula de Innovación	Acceso no autorizado a utilizar laptop del aula	NO	Insatisfecho	seguridad información
20/12/2023	Laptop	Aula de Innovación	Acceso no autorizado a utilizar laptop del aula	NO	Insatisfecho	seguridad información
20/12/2023	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Insatisfecho	riesgo informático
20/12/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°45	NO	Insatisfecho	riesgo informático
22/12/2023	Sistema operativo	Aula 01	Error en la activación del producto en laptop N°41	NO	Insatisfecho	control informático
22/12/2023	Sistema operativo	Aula 01	Error en la activación del producto en laptop N°46	NO	Insatisfecho	control informático
22/12/2023	Sistema operativo	Aula 01	Error en la activación del producto en laptop N°50	NO	Insatisfecho	control informático
22/12/2023	Sistema operativo	Aula 01	Error en la activación del producto en laptop N°56	NO	Insatisfecho	control informático
22/12/2023	Laptop	Aula de Innovación	Acceso no autorizado a utilizar laptop del aula	NO	Insatisfecho	seguridad información
22/12/2023	Laptop	Aula 04	Laptop no proyecta imagen en el proyector	SI	Neutral	riesgo informático
22/12/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°56	SI	Satisfecho	riesgo informático
22/12/2023	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Insatisfecho	riesgo informático
26/12/2023	Contraseñas	Dirección	Contraseña del SIAGIE quedo guardada en el navegador de internet	SI	Neutral	riesgo informático
26/12/2023	Laptop	Aula de Innovación	Troyano encontrado en la laptop N°25	SI	Insatisfecho	riesgo informático
26/12/2023	Contraseñas	Aula 04	Inicio de sesión no autorizada en laptop N°76	NO	Insatisfecho	seguridad información
26/12/2023	Laptop	Aula de Innovación	Acceso no autorizado a utilizar laptop del aula	NO	Insatisfecho	seguridad información
26/12/2023	Proyector	Dirección	Error en configuración del proyector	SI	Satisfecho	control informático
26/12/2023	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Insatisfecho	riesgo informático
26/12/2023	Laptop	Coord. Ciencias	Error de configuración wifi	SI	Satisfecho	control informático
26/12/2023	Laptop	Coord. Letras	Acceso no autorizado a utilizar laptop del aula	NO	Insatisfecho	seguridad información
26/12/2023	Boleta de notas	Dirección	Pérdida de boletas de notas de tres estudiantes	SI	Insatisfecho	seguridad información

26/12/2023	PAT	Dirección	Pérdida de PATs de años anteriores	NO	Completamente Insatisfecho	seguridad información
29/12/2023	Laptop	Aula de Innovación	Acceso no autorizado a utilizar laptop 11 del aula	NO	Insatisfecho	seguridad información
29/12/2023	Laptop	Aula de Innovación	Acceso no autorizado a utilizar laptop 14 del aula	NO	Insatisfecho	seguridad información
29/12/2023	Laptop	Aula de Innovación	Acceso no autorizado a utilizar laptop 15 del aula	NO	Insatisfecho	seguridad información
29/12/2023	Office	Dirección	Falta el código de activación del producto	SI	Satisfecho	control informático
3/01/2024	Boleta de notas	Dirección	Pérdida de boletas de notas del 2021	SI	Completamente Insatisfecho	seguridad información
3/01/2024	Memorandums	Dirección	Pérdida de memorandums digitales del 2020	NO	Completamente Insatisfecho	seguridad información
3/01/2024	Laptop	Aula de Innovación	Pérdida de una laptop del aula de innovación	NO	Completamente Insatisfecho	seguridad información
3/01/2024	Disco duro externo	Dirección	Pérdida de backups de restauración de SO	SI	Completamente Insatisfecho	seguridad información
3/01/2024	Disco duro externo	Dirección	Pérdida de inventario de años anteriores	NO	Completamente Insatisfecho	seguridad información
4/01/2024	Contraseñas	Aula de Innovación	Docente olvidó su contraseña de inicio de sesión de su correo	SI	Satisfecho	riesgo informático
4/01/2024	Boleta de notas	Dirección	Plataforma SIAGIE aun no permite validar boletas de notas	NO	Insatisfecho	riesgo informático
4/01/2024	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Insatisfecho	riesgo informático
10/01/2024	Office	Dirección	Falta el código de activación del producto	SI	Satisfecho	control informático
10/01/2024	Laptop	Aula de Innovación	Error de actualización de drivers	NO	Insatisfecho	control informático
10/01/2024	Laptop	Aula de Innovación	Error de actualización de drivers	NO	Insatisfecho	control informático
10/01/2024	Laptop	Aula de Innovación	Error de actualización de drivers	NO	Insatisfecho	control informático
10/01/2024	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Insatisfecho	riesgo informático
10/01/2024	Laptop	Aula de Innovación	Infección de virus por usb	SI	Neutral	riesgo informático
10/01/2024	Estabilizador	Dirección	Estabilizador malogrado por fuerte descarga eléctrica	NO	Insatisfecho	riesgo informático
17/01/2024	Laptop	Aula de Innovación	Error de actualización de drivers	NO	Insatisfecho	control informático

18/01/2024	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Insatisfecho	riesgo informático
19/01/2024	Laptop	Aula de Innovación	Infección de virus por usb	SI	Neutral	riesgo informático
22/01/2024	Laptop	Aula de Innovación	Error de actualización de drivers en laptop	NO	Insatisfecho	control informático
23/01/2024	Laptop	Aula de Innovación	Error de actualización de drivers en laptop	NO	Insatisfecho	control informático
24/01/2024	Armario de metal	Dirección	No se encuentra la llave para abrir el armario	SI	Satisfecho	riesgo informático
25/01/2024	PC	Coord. Tutotía	No se encuentra drives para actualizar	NO	Insatisfecho	riesgo informático
26/01/2024	Laptop	Aula de Innovación	Error de actualización de drivers	NO	Insatisfecho	control informático
29/01/2024	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Insatisfecho	riesgo informático
30/01/2024	Disco duro externo	Aula de Innovación	Almacenamiento casi lleno del disco, urgencia de comprar uno nuevo o borrar datos	SI	Satisfecho	riesgo informático
31/01/2024	Laptop	Aula de Innovación	Infección de virus por usb	SI	Neutral	riesgo informático
1/02/2024	Reproductor de video	Dirección	Reproductor de video encontrado en completo estado de suciedad	SI	Satisfecho	riesgo informático
2/02/2024	Ficha de monitoreo	Coord. Letras	Daños a las fichas de monitoreo por ingreso de lluvia en el local	NO	Insatisfecho	seguridad información
5/02/2024	Router	Dirección	Router se para desconfigurando cada que se va la luz	SI	Insatisfecho	riesgo informático
6/02/2024	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Insatisfecho	riesgo informático
7/02/2024	Cámara de vigilancia	Almacén	Se encontró cámaras de vigilancia sin inventario	SI	Satisfecho	control informático
8/02/2024	Laptop	Aula de Innovación	Infección de virus por usb	SI	Neutral	riesgo informático
9/02/2024	Laptop	Aula de Innovación	Error de actualización de drivers	NO	Insatisfecho	control informático
12/02/2024	PC	Almacén	Equipos desfasados almacenados sin inventario	NO	Insatisfecho	seguridad información
13/02/2024	Equipo de sonido	Dirección	Se repara con un técnico el equipo de sonido	SI	Satisfecho	control informático
14/02/2024	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Insatisfecho	riesgo informático
15/02/2024	Amplificador de audio	Almacén	Equipos almacenados sin inventario, se agrega al inventario	SI	Satisfecho	seguridad información
15/02/2024	Router	Almacén	Equipo almacenados sin inventario, se agrega al inventario	SI	Satisfecho	seguridad información
15/02/2024	Televisor	Almacén	Equipo almacenados sin inventario, se agregar al inventario	SI	Satisfecho	seguridad información
15/02/2024	Proyector	Almacén	Equipo almacenados sin inventario, se agrega al inventario	SI	Satisfecho	seguridad información

15/02/2024	Sistema operativo	Aula de Innovación	Actualización de sistema operativo a la versión Windows 10 laptop del 1 al 20	SI	Satisfecho	control informático
15/02/2024	Sistema operativo	Aula de Innovación	Actualización de sistema operativo a la versión Windows 10 laptop del 21 al 30	SI	Satisfecho	control informático
15/02/2024	Sistema operativo	Aula de Innovación	Actualización de sistema operativo a la versión Windows 10 laptop del 31 al 40	SI	Satisfecho	control informático
15/02/2024	Sistema operativo	Dirección	Laptop dañada no se puede reparar	NO	Insatisfecho	control informático
15/02/2024	Sistema operativo	Aula de Innovación	Laptop 25 batería malograda, se requiere reparación	SI	Satisfecho	riesgo informático
15/02/2024	Sistema operativo	Aula de Innovación	Laptop 13 no se encuentra cargador	NO	Insatisfecho	riesgo informático
16/02/2024	Laptop	Aula 01	Acceso no autorizado a utilizar laptop del aula	NO	Insatisfecho	seguridad información
16/02/2024	Laptop	Aula de Innovación	Acceso no autorizado a utilizar laptop del aula, cerradura arreglada	SI	Satisfecho	seguridad información
16/02/2024	Sistema operativo	Aula 01	Actualización de sistema operativo a la versión Windows 10	SI	Satisfecho	control informático
16/02/2024	Sistema operativo	Aula 01	Actualización de sistema operativo a la versión Windows 10	SI	Satisfecho	control informático
16/02/2024	Laptop	Aula 01	Laptop 43 no se encuentra cargador	SI	Satisfecho	riesgo informático
16/02/2024	Laptop	Aula 01	Laptop 54 no se encuentra cargador	SI	Satisfecho	riesgo informático
19/02/2024	PC	Almacén	Se agrega al inventario institucional las PCs guardadas	SI	Satisfecho	seguridad información
19/02/2024	Estabilizador	Almacén	Se agrega al inventario institucional	SI	Satisfecho	seguridad información
19/02/2024	Equipo de sonido	Almacén	Se agrega al inventario institucional	SI	Satisfecho	seguridad información
19/02/2024	Laptop	Aula 01	Laptop 63 se daña por fuerte descarga electrica	NO	Insatisfecho	riesgo informático
19/02/2024	Laptop	Aula 01	Laptop 70 se daña por fuerte descarga electrica	SI	Satisfecho	riesgo informático
19/02/2024	Laptop	Aula 01	no se cuenta con capacitación para uso de equipos en momentos de tormentas ambientales	NO	Insatisfecho	control informático
19/02/2024	Laptop	Aula 01	se realiza capacitacion para uso de equipos en momentos de tormentas ambientales	SI	Satisfecho	control informático
20/02/2024	Laptop	Aula 06	se soluciona problema de acceso con vigilancia del personal autorizado	SI	Satisfecho	seguridad información
20/02/2024	Laptop	Aula de Innovación	Se Instala programa Deepfreezer para evitar errores de configuración laptop del 1 al 20	SI	Satisfecho	control informático
20/02/2024	Laptop	Aula de Innovación	Se Instala programa Deepfreezer para evitar errores de configuración laptop del 21 al 30	SI	Satisfecho	control informático
20/02/2024	Laptop	Aula de Innovación	Se Instala programa Deepfreezer para evitar errores de configuración laptop del 31 al 40	SI	Satisfecho	control informático

20/02/2024	Laptop	Dirección	se encuentra virus en laptop	NO	Insatisfecho	riesgo informático
20/02/2024	Laptop	Dirección	se instala programa antivirus en laptop	SI	Satisfecho	riesgo informático
20/02/2024	Laptop	Aula 01	Acceso no autorizado a utilizar laptop del aula	NO	Insatisfecho	seguridad información
20/02/2024	Laptop	Aula 01	se soluciona problema de acceso con vigilancia del personal autorizado	SI	Satisfecho	seguridad información
21/02/2024	Laptop	Aula 01	Se Instala programa Deepfreezer para evitar errores de configuración laptop del 41 al 55	SI	Satisfecho	control informático
21/02/2024	Laptop	Aula 01	Se Instala programa Deepfreezer para evitar errores de configuración laptop del 56 al 60	SI	Satisfecho	control informático
21/02/2024	Laptop	Aula 01	Se Instala programa Deepfreezer para evitar errores de configuración laptop del 61 al 70	SI	Satisfecho	control informático
21/02/2024	Laptop	Caseta auxiliar	se encuentra virus en laptop	NO	Insatisfecho	riesgo informático
21/02/2024	Laptop	Caseta auxiliar	se instala programa antivirus en laptop	SI	Satisfecho	riesgo informático
21/02/2024	Laptop	Caseta auxiliar	Acceso no autorizado a utilizar laptop del aula	SI	Satisfecho	seguridad información
21/02/2024	Laptop	Caseta auxiliar	se soluciona problema de acceso con vigilancia del personal autorizado	SI	Satisfecho	seguridad información
22/02/2024	Laptop	Coord. Ciencias	se encuentra virus en laptop	NO	Insatisfecho	riesgo informático
22/02/2024	Laptop	Coord. Ciencias	se instala programa antivirus en laptop	SI	Satisfecho	riesgo informático
22/02/2024	Laptop	Coord. Ciencias	Acceso no autorizado a utilizar laptop del aula	SI	Satisfecho	seguridad información
22/02/2024	Laptop	Coord. Ciencias	se soluciona problema de acceso con vigilancia del personal autorizado	SI	Satisfecho	seguridad información
22/02/2024	Laptop	Coord. Ciencias	Se Instala programa Deepfreezer para evitar errores de configuración	SI	Satisfecho	control informático
22/02/2024	Laptop	Dirección	Se Instala programa Deepfreezer para evitar errores de configuración	SI	Satisfecho	control informático
22/02/2024	Laptop	Coord. Tutotía	Se Instala programa Deepfreezer para evitar errores de configuración	SI	Satisfecho	control informático
22/02/2024	Laptop	Coord. Letras	Se Instala programa Deepfreezer para evitar errores de configuración	SI	Satisfecho	control informático
23/02/2024	Laptop	Coord. Letras	se encuentra virus en laptop	NO	Insatisfecho	riesgo informático
23/02/2024	Laptop	Coord. Letras	se instala programa antivirus en laptop	SI	Satisfecho	riesgo informático
23/02/2024	Laptop	Coord. Letras	Acceso no autorizado a utilizar laptop del aula	NO	Insatisfecho	seguridad información

23/02/2024	Laptop	Coord. Letras	se soluciona problema de acceso con vigilancia del personal autorizado	SI	Satisfecho	seguridad información
23/02/2024	Laptop	Caseta auxiliar	Se Instala programa Deepfreezer para evitar errores de configuración	SI	Satisfecho	control informático
23/02/2024	PC	Dirección	Se Instala programa Deepfreezer para evitar errores de configuración	SI	Satisfecho	control informático
26/02/2024	Laptop	Aula 10	Acceso no autorizado a utilizar laptop del aula	NO	Insatisfecho	seguridad información
26/02/2024	Laptop	Aula 10	se soluciona problema de acceso con vigilancia del personal autorizado	SI	Satisfecho	seguridad información
26/02/2024	Laptop	Aula 10	Se Instala programa Deepfreezer para evitar errores de configuración	SI	Satisfecho	control informático
26/02/2024	Laptop	Dirección	Se Instala programa Deepfreezer para evitar errores de configuración	SI	Satisfecho	control informático
26/02/2024	Laptop	Coord. Tutotía	Se aplica antivirus a todas las computadoras y laptops	SI	Satisfecho	riesgo informático
26/02/2024	Laptop	Coord. Letras	Se aplica antivirus a todas las computadoras y laptops	SI	Satisfecho	riesgo informático
26/02/2024	Armario de metal	Aula de Innovación	Se soluciono problema de cerradura del armario donde se almacenan las laptops	SI	Satisfecho	seguridad información
27/02/2024	Laptop	Aula de Innovación	Se aplica antivirus a todas las computadoras y laptops del 1 al 15	SI	Satisfecho	riesgo informático
27/02/2024	Laptop	Aula de Innovación	Se aplica antivirus a todas las computadoras y laptops del 16 al 29	SI	Satisfecho	riesgo informático
27/02/2024	Laptop	Aula de Innovación	Se aplica antivirus a todas las computadoras y laptops del 30 al 40	SI	Satisfecho	riesgo informático
27/02/2024	Laptop	Aula de Innovación	cambios en la configuración de la laptop 17	SI	Satisfecho	control informático
27/02/2024	Laptop	Aula de Innovación	error de actualización de SO laptop 37	NO	Insatisfecho	control informático
27/02/2024	Laptop	Coord. Letras	Acceso no autorizado a utilizar laptop del aula	NO	Insatisfecho	seguridad información
27/02/2024	Laptop	Coord. Letras	se soluciona problema de acceso con vigilancia del personal autorizado	SI	Satisfecho	seguridad información
27/02/2024	Contraseñas	Dirección	secretaria dejo guardada su contraseña en el navegador	SI	Satisfecho	seguridad información
27/02/2024	Contraseñas	Dirección	director dejo abierto su whatsapp personal	SI	Satisfecho	seguridad información
28/02/2024	Laptop	Aula 01	Se aplica antivirus a todas las computadoras y laptops del 41 al 55	SI	Satisfecho	riesgo informático
28/02/2024	Laptop	Aula 01	Se aplica antivirus a todas las computadoras y laptops del 56 al 65	SI	Satisfecho	riesgo informático
28/02/2024	Laptop	Aula 01	Se aplica antivirus a todas las computadoras y laptops del 66 al 70	SI	Satisfecho	riesgo informático
28/02/2024	Laptop	Dirección	se encuentra virus en laptop	NO	Insatisfecho	riesgo informático
28/02/2024	Laptop	Dirección	se instala programa antivirus en laptop	SI	Satisfecho	riesgo informático

28/02/2024	Contraseñas	Dirección	Contraseña del SIAGIE quedo guardada en el navegador de internet	SI	Satisfecho	seguridad información
28/02/2024	Laptop	Aula 01	Acceso no autorizado a utilizar laptop del aula	NO	Insatisfecho	seguridad información
28/02/2024	Laptop	Aula 01	se soluciona problema de acceso con vigilancia del personal autorizado	SI	Satisfecho	seguridad información
29/02/2024	Laptop	Dirección	Se aplica antivirus a computadora direccion 1	SI	Satisfecho	riesgo informático
29/02/2024	Laptop	Dirección	Se aplica antivirus a computadora direccion 2	SI	Satisfecho	riesgo informático
29/02/2024	Laptop	Dirección	se implementa las políticas de seguridad aceptadas por dirección	SI	Satisfecho	seguridad información
29/02/2024	Laptop	Aula de Innovación	se implementa las políticas de seguridad aceptadas por dirección	SI	Satisfecho	seguridad información
29/02/2024	Laptop	Dirección	fuertes descargas electricas por tormenta ocurrida	NO	Insatisfecho	riesgo informático
29/02/2024	Laptop	Aula de Innovación	se compra UPS para proteger laptops del 1 al 6	SI	Satisfecho	riesgo informático
29/02/2024	Fotocopiadora	Dirección	error de configuración del equipo	NO	Neutral	control informático
29/02/2024	Fotocopiadora	Dirección	se brinda capacitación sobre buen uso	SI	Satisfecho	control informático
29/02/2024	Impresora	Dirección	se brinda capacitación sobre buen uso	SI	Satisfecho	control informático
1/03/2024	Contraseñas	Aula de Innovación	Docente olvidó su contraseña de inicio de sesión de su correo	SI	Satisfecho	riesgo informático
1/03/2024	Contraseñas	Aula de Innovación	Capacitación sobre craación de contraseñas seguras	SI	Satisfecho	control informático
1/03/2024	Laptop	Aula de Innovación	Capacitación del mantenimiento y configuración de las impresoras	SI	Satisfecho	control informático
1/03/2024	Laptop	Aula 01	Capacitación del mantenimiento y configuración de las laptops	SI	Satisfecho	control informático
1/03/2024	Laptop	Aula 04	Infección de virus por usb	SI	Neutral	riesgo informático
1/03/2024	Disco duro externo	Aula de Innovación	Perdida de información sobre software educativo	SI	Satisfecho	seguridad información
1/03/2024	Disco duro externo	Aula de Innovación	Información de datos personales de los docentes encontrados sin protección	SI	Satisfecho	seguridad información
4/03/2024	Armario de metal	Aula 01	Se soluciono problema de cerradura del armario donde se almacenan las laptops	SI	Satisfecho	seguridad información
4/03/2024	PAT	Dirección	No se encuentra el PAT del año pasado	NO	Insatisfecho	seguridad información
4/03/2024	PAT	Dirección	Se hace una copia de respaldo del PAT actual	SI	Satisfecho	seguridad información
4/03/2024	Contraseñas	Aula de Innovación	Docente olvidó su contraseña de inicio de sesión de su correo	SI	Satisfecho	riesgo informático
4/03/2024	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Neutral	riesgo informático

5/03/2024	RIN	Dirección	RIN anteriores no se encuentran almacenados de manera física	NO	Insatisfecho	riesgo informático
5/03/2024	Router	Dirección	Se compró UPS para controlar el router y proteger de cortes de energía	SI	Satisfecho	riesgo informático
5/03/2024	Laptop	Aula de Innovación	Se compró UPS para proteger de cortes de energía	SI	Satisfecho	riesgo informático
5/03/2024	Sistema operativo	Aula de Innovación	Se hace una copia de respaldo	SI	Satisfecho	seguridad información
5/03/2024	Reg. Asistencia trabajadores	Dirección	Se hace una copia de respaldo	SI	Satisfecho	seguridad información
5/03/2024	Reg. Asistencia estudiantes	Caseta auxiliar	Se hace una copia de respaldo	SI	Satisfecho	seguridad información
5/03/2024	PAT	Dirección	Se crea correo institucional para respaldar archivos digitales	SI	Satisfecho	control informático
5/03/2024	Ficha de monitoreo	Dirección	Se crea correo institucional para respaldar archivos digitales	SI	Satisfecho	control informático
5/03/2024	Boleta de notas	Dirección	Se crea correo institucional para respaldar archivos digitales	NO	Insatisfecho	control informático
5/03/2024	Laptop	Aula de Innovación	se crea herramienta de incidencias	SI	Satisfecho	control informático
6/03/2024	RIN	Dirección	No se encuentra el RIN del año pasado	NO	Insatisfecho	seguridad información
6/03/2024	RIN	Dirección	Se hace una copia de respaldo del RIN actual	SI	Satisfecho	seguridad información
6/03/2024	Memorandums	Dirección	Se hace una copia de respaldo	SI	Satisfecho	seguridad información
6/03/2024	Proyector	Almacén	Se encuentra en almacen el manual de uso para configuración del router	SI	Satisfecho	control informático
6/03/2024	Equipo de sonido	Almacén	Se encuentra en almacen el manual de uso para configuración del router	SI	Satisfecho	control informático
6/03/2024	Laptop	Almacén	Se encuentra en almacen el manual de uso para configuración del router	SI	Satisfecho	control informático
6/03/2024	Router	Almacén	Se encuentra en almacen el manual de uso para configuración del router	NO	Neutral	control informático
6/03/2024	Laptop	Aula de Innovación	Lentitud del equipo n22 por ser obsoleto	NO	Insatisfecho	riesgo informático
6/03/2024	Laptop	Dirección	Lentitud del equipo n3 por ser obsoleto	SI	Satisfecho	riesgo informático
6/03/2024	Laptop	Dirección	Lentitud del equipo n4 por ser obsoleto	SI	Satisfecho	riesgo informático
6/03/2024	Impresora	Dirección	Obstrucción de papel en la copiadora	SI	Satisfecho	riesgo informático
6/03/2024	Reproductor de video	Dirección	cable de alimentación roto	SI	Satisfecho	riesgo informático
8/03/2024	Contraseñas	Aula de Innovación	Capacitación del uso del programa BitWarden para gestión de contraseñas	SI	Satisfecho	control informático

8/03/2024	Laptop	Aula de Innovación	Capacitación del mantenimiento y configuración de las laptops	SI	Satisfecho	control informático
8/03/2024	Fotocopiadora	Dirección	Obstrucción de papel en la copiadora	SI	Satisfecho	riesgo informático
8/03/2024	Contraseñas	Coord. Letras	Capacitación del uso del programa BitWarden para gestión de contraseñas	SI	Satisfecho	control informático
8/03/2024	Laptop	Coord. Letras	Capacitación del mantenimiento y configuración de las laptops	SI	Satisfecho	control informático
8/03/2024	Contraseñas	Coord. Ciencias	Capacitación del uso del programa BitWarden para gestión de contraseñas	SI	Satisfecho	control informático
8/03/2024	Contraseñas	Dirección	secretaria no recuerda la nueva contraseña creada para acceso al SIAGIE	SI	Satisfecho	riesgo informático
8/03/2024	Amplificador de audio	Dirección	equipo expuesto a fuertes lluvias por uso en patio al aire libre	NO	Insatisfecho	riesgo informático
8/03/2024	Estabilizador	Aula 01	cable de alimentación deteriorado	SI	Satisfecho	riesgo informático
8/03/2024	Proyector	Aula 03	acceso al aula sin autorización, personal de vigilancia anotó datos de estudiante	SI	Satisfecho	seguridad información
8/03/2024	Proyector	Aula 05	acceso al aula sin autorización, cerradura malograda	NO	Insatisfecho	seguridad información
8/03/2024	Laptop	Coord. Ciencias	Capacitación del mantenimiento y configuración de las laptops	SI	Satisfecho	control informático
8/03/2024	Contraseñas	Coord. Tutotía	Capacitación del uso del programa BitWarden para gestión de contraseñas	SI	Satisfecho	control informático
8/03/2024	Laptop	Coord. Tutotía	Capacitación del mantenimiento y configuración de las laptops	SI	Satisfecho	control informático
8/03/2024	Laptop	Aula de Innovación	Capacitación del uso de internet y tipos de virus	SI	Satisfecho	control informático

Ficha de registros

Ficha de registro Pre Test para seguridad de la información

Investigador:	Mateo Condor Kevin Rolando			
Institución educativa:	I.E. “Francisco de Zela”			
Dirección:	Jr. Rosario N°632			
Fecha de inicio:	27/11/2023			
Fecha de terminación:	03/01/2024			
Variable:	Formula:			
Reportes:		$SI = \frac{RAS}{TAS} X100$		
Indicador:	Medida	Donde:		
Seguridad de la información (pre test)	Porcentaje	Donde: SI: Seguridad de información TAS: Total de accesos de seguridad de información RAS: Reporte de accesos solucionados al día		
Ítem	Fecha	RAS	TAS	SI
1	27/11/2023	2	3	67%
2	28/11/2023	1	2	50%
3	29/11/2023	3	4	75%
4	30/11/2023	4	5	80%
5	1/12/2023	2	3	67%
6	5/12/2023	3	4	75%
7	6/12/2023	2	2	100%
8	7/12/2023	4	5	80%
9	11/12/2023	2	2	100%
10	13/12/2023	2	3	67%
11	15/12/2023	2	3	67%
12	19/12/2023	2	2	100%
13	20/12/2023	2	3	67%
14	26/12/2023	4	5	80%
15	29/12/2024	2	3	67%
16	3/01/2024	3	5	60%
	TOTAL	40	54	
	PROMEDIO			75%

Ficha de registro Post test para seguridad de la información

Investigador:	Mateo Condor Kevin Rolando			
Institución educativa:	I.E. “Francisco de Zela”			
Dirección:	Jr. Rosario N°632			
Fecha de inicio:	15/02/2024			
Fecha de terminación:	08/03/2024			
Variable:	Formula:			
Reportes:		$SI = \frac{RAS}{TAS} X100$		
Indicador	Medida	Donde: SI: Seguridad de información TAS: Total de accesos de seguridad de información RAS: Reporte de accesos solucionados al día		
Seguridad de la información (post test)	Porcentaje			
Ítem	Fecha	RAS	TAS	SI
1	15/02/2024	0	4	0%
2	16/02/2024	1	2	50%
3	19/02/2024	0	3	0%
4	20/02/2024	1	3	33%
5	21/02/2024	0	2	0%
6	22/02/2024	0	2	0%
7	23/02/2024	1	2	50%
8	26/02/2024	1	3	33%
9	27/02/2024	1	4	25%
10	28/02/2024	1	3	33%
11	29/02/2024	0	2	0%
12	01/03/2024	0	2	0%
13	04/03/2024	1	3	33%
14	05/03/2024	0	3	0%
15	06/03/2024	1	3	33%
16	08/03/2024	1	2	50%
	TOTAL	9	43	
	PROMEDIO			21%

Ficha de registro Pre Test para riesgo informático

Investigador:	Mateo Condor Kevin Rolando			
Institución educativa:	I.E. “Francisco de Zela”			
Dirección:	Jr. Rosario N°632			
Fecha de inicio:	27/11/2023			
Fecha de terminación:	04/01/2024			
Variable:	Formula:			
Reportes:		$RDI = \frac{RRDI}{TRDI} x100$		
Indicador	Medida	Donde: RDI: Riesgo de la Información RRDI: Reporte de riesgos de información solucionados al día TRDI: Total de riesgo de la información al día		
Riesgo informático (pre test)	Porcentaje			
Ítem	Fecha	RRDI	TRDI	RDI%
1	27/11/2023	8	11	73%
2	29/11/2023	4	6	67%
3	30/11/2023	1	1	100%
4	1/12/2023	5	6	83%
5	4/12/2023	3	4	75%
6	6/12/2023	2	3	67%
7	7/12/2023	2	3	67%
8	8/12/2023	1	2	50%
9	11/12/2023	1	2	50%
10	12/12/2023	2	3	67%
11	14/12/2023	2	3	67%
12	19/12/2023	2	3	67%
13	20/12/2023	1	2	50%
14	22/12/2023	2	3	67%
15	26/12/2024	2	3	67%
16	4/01/2024	2	3	67%
	TOTAL	**40**	**58**	
	PROMEDIO			**68%**

Ficha de registro Post test para riesgo informático

Investigador:	Mateo Condor Kevin Rolando			
Institución educativa:	I.E. “Francisco de Zela”			
Dirección:	Jr. Rosario N°632			
Fecha de inicio:	15/02/2024			
Fecha de terminación:	08/03/2024			
Variable:	Formula:			
Reportes:		$RDI = \frac{RRDI}{TRDI} x100$ Donde: RDI: Riesgo de la Información RRDI: Reporte de riesgos de información solucionados al día TRDI: Total de riesgo de la información al día		
Indicador	Medida			
Riesgo informático acción (post test)	Porcentaje			
Ítem	Fecha	RRDI	TRDI	RDI%
1	15/02/2024	1	4	25%
2	16/02/2024	0	2	0%
3	19/02/2024	1	2	50%
4	20/02/2024	1	2	50%
5	21/02/2024	1	2	50%
6	22/02/2024	1	2	50%
7	23/02/2024	1	2	50%
8	26/02/2024	0	2	0%
9	27/02/2024	0	3	0%
10	28/02/2024	1	5	20%
11	29/02/2024	1	4	25%
12	01/03/2024	0	2	0%
13	04/03/2024	0	2	0%
14	05/03/2024	1	3	33%
15	06/03/2024	1	5	20%
16	08/03/2024	1	4	25%
	TOTAL	11	46	
	PROMEDIO			25%

Ficha de registro Pre Test para control informático

Investigador:	Mateo Condor Kevin Rolando			
Institución educativa:	I.E. “Francisco de Zela”			
Dirección:	Jr. Rosario N°632			
Fecha de inicio:	28/11/2023			
Fecha de terminación:	10/01/2024			
Variable:	Formula:			
Reportes:		$IC = \frac{TIC}{TICD} x100$		
Indicador	Medida	Donde: IC: Control informático TIC: Total controles informáticos TCID: Total de controles aplicados al día		
Control informático (pre test)	Porcentaje			
Ítem	Fecha	TIC	TCID	IC%
1	28/11/2023	3	5	60%
2	29/11/2023	3	4	75%
3	30/11/2023	1	1	100%
4	4/12/2023	2	3	67%
5	6/12/2023	1	1	100%
6	7/12/2023	2	3	67%
7	8/12/2023	1	1	100%
8	12/12/2023	4	5	80%
9	13/12/2023	1	2	50%
10	15/12/2023	1	2	50%
11	19/12/2023	1	2	50%
12	22/12/2023	3	4	75%
13	26/12/2023	1	2	50%
14	10/01/2024	3	4	75%
	TOTAL	27	39	
	PROMEDIO			71%

Ficha de registro Post test para control informático

Investigador:	Mateo Condor Kevin Rolando			
Institución educativa:	I.E. “Francisco de Zela”			
Dirección:	Jr. Rosario N°632			
Fecha de inicio:	15/02/2024			
Fecha de terminación:	08/03/2024			
Variable:	Formula:			
Reportes:		$IC = \frac{TIC}{TICD} x100$		
Indicador	Medida	Donde: IC: Control informático TIC: Total controles informáticos TCID: Total de controles aplicados al día		
Control informático (post test)	Porcentaje			
Ítem	Fecha	TIC	TCID	IC%
1	15/02/2024	1	3	33%
2	16/02/2024	0	2	0%
3	19/02/2024	1	2	50%
4	20/02/2024	0	3	0%
5	21/02/2024	0	3	0%
6	22/02/2024	0	4	0%
7	23/02/2024	0	2	0%
8	26/02/2024	0	2	0%
9	27/02/2024	1	2	50%
10	29/02/2024	1	3	33%
11	01/03/2024	0	3	0%
12	05/03/2024	1	4	25%
13	06/03/2024	1	4	25%
14	08/03/2024	0	9	0%
	TOTAL	6	46	
	PROMEDIO			15%

Anexo 07. Consentimiento Informado

CONSENTIMIENTO INFORMADO PARA PARTICIPANTES DEL PROYECTO DE INVESTIGACIÓN

N° 001

El propósito de esta ficha de consentimiento es proveer a los participantes en esta investigación una clara explicación de la naturaleza de la misma, así como su rol en ella, como participantes del proyecto de investigación titulado: "SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA MEJORAR LA SEGURIDAD INFORMÁTICA DE LA I.E. FRANCISCO DE ZELA – HUANCAYO - 2024".

La presente investigación es conducida por: MATEO CONDOR, Kevin Rolando. Bachiller de la facultad de Ingeniería de la Universidad Peruana Los Andes. El **objetivo** de este estudio es: Determinar en qué medida el sistema de gestión de la seguridad de la información favorece la seguridad informática de la I.E. Francisco de Zela.

Si usted accede a participar en este estudio, se le pedirá desarrollar una encuesta según el tema. Esto tomará aproximadamente 10 minutos de su tiempo.

La información que se recoja será confidencial y no se usará para ningún otro propósito fuera de esta investigación. Sus respuestas al cuestionario serán codificadas usando un número de identificación y, por lo tanto, serán anónimas.

Desde ya le agradecemos su participación.

Anexo 07. Autorización para realizar trabajo de investigación

PERÚ | MINISTERIO DE EDUCACIÓN | DRE JUNIN | UGEL HUANCAYO | INSTITUCION EDUCATIVA "FRANCISCO DE ZELA"

AUTORIZACIÓN PARA REALIZAR TRABAJO DE INVESTIGACIÓN

DATOS GENERALES

NOMBRE DE LA ORGANIZACIÓN		RUC
INSTITUCIÓN EDUCATIVA PÚBLICA FRANCISCO DE ZELA		
PROVINCIA	**DISTRITO**	**CÓDIGO MODULAR**
HUANCAYO	EL TAMBO	0919308

CONSENTIMIENTO

De conformidad con lo establecido en la Institución Educativa, autorizo para desarrollar el trabajo de investigación. Le concedemos acceso a los recursos y las instalaciones necesarias de la I.E. Francisco de Zela para llevar a cabo su investigación. Asimismo, le otorgamos permiso para realizar actividades relacionadas con su tesis, incluyendo entrevistas, encuestas u otras investigaciones pertinentes.

NOMBRE DEL TRABAJO DE INVESTIGACIÓN	
Sistema de Gestión de la Seguridad de la Información para mejorar la Seguridad Informática del colegio Francisco de Zela	
NOMBRE DEL PROGRAMA ACADÉMICO	
Escuela Profesional de Ingeniería de Sistemas y Computación	
AUTOR	**DNI**
Mateo Condor Kevin Rolando	70239758

Le recordamos lo importante que es seguir todas las normas y políticas marcadas por nuestra institución durante el proceso de investigación y desarrollo. Siempre estamos listos para responder cualquier pregunta o aclaración adicional que pueda necesitar durante el proceso de tesis.

Felicitaciones por ingresar a esta fase académica y mucha suerte con su proyecto.

Huancayo, 22 de diciembre del 2023

Lic. M. Rosario Gavilan N.
C.M. 1019912052
DIRECTORA

Milagro Rosario Gavilan Hilario

DIRECTORA

Anexo 06. Evidencias Fotográficas

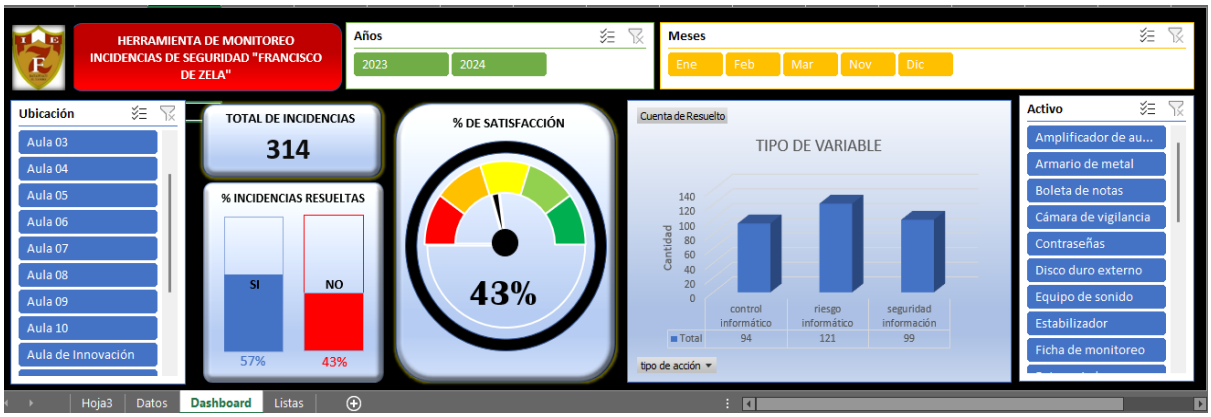

Fig. 27. Dashboard de monitoreo de incidencias.

Fig. 28. Armario de metal con orden de numeración para laptops

Fig. 29. Instalación de UPS para aula de innovación.

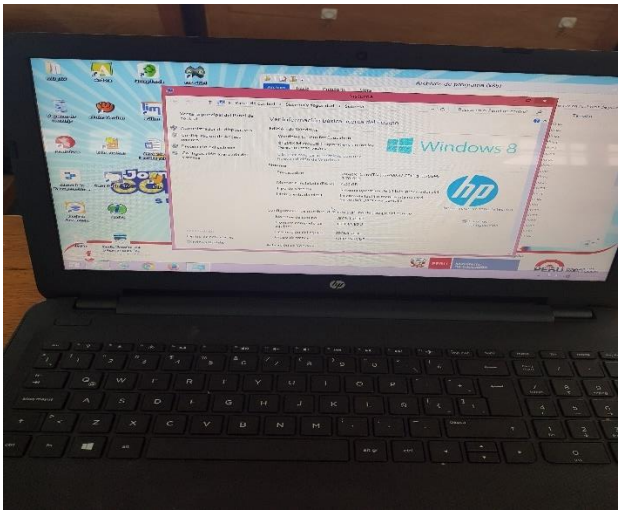

Fig. 30. Actualización de software de equipos.

Fig. 31. Instalación de Software antivirus y antimalware.

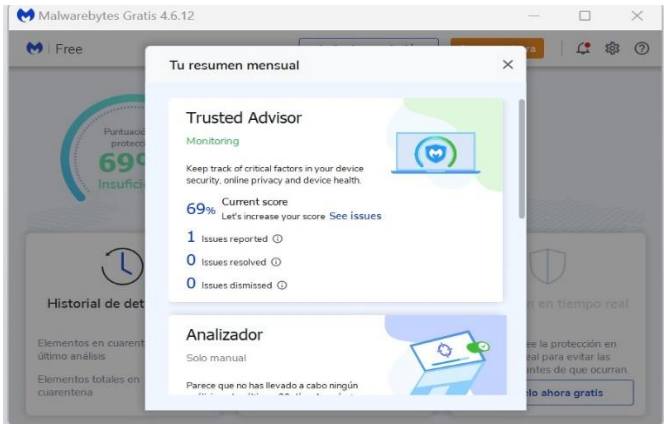

Fig. 32. Revisión Semanal de protección contra virus.

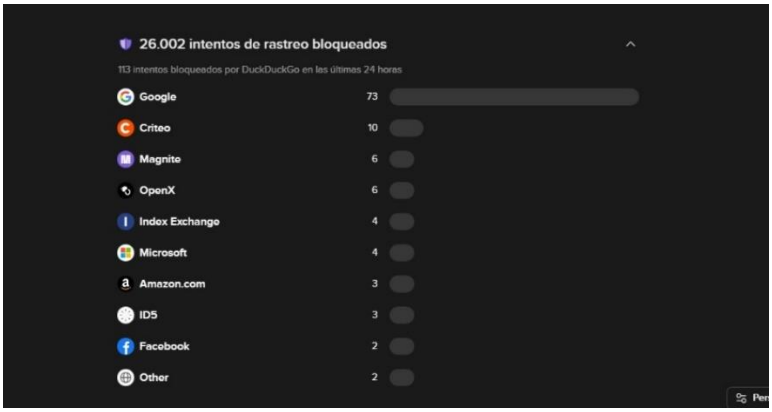

Fig. 33. Bloqueo de rastreo de datos.

Fig. 34. Cerradura para puerta principal del aula de innovación.

Fig. 35. Clasificación de archivos de información.
Fuente. Elaboración Propia.

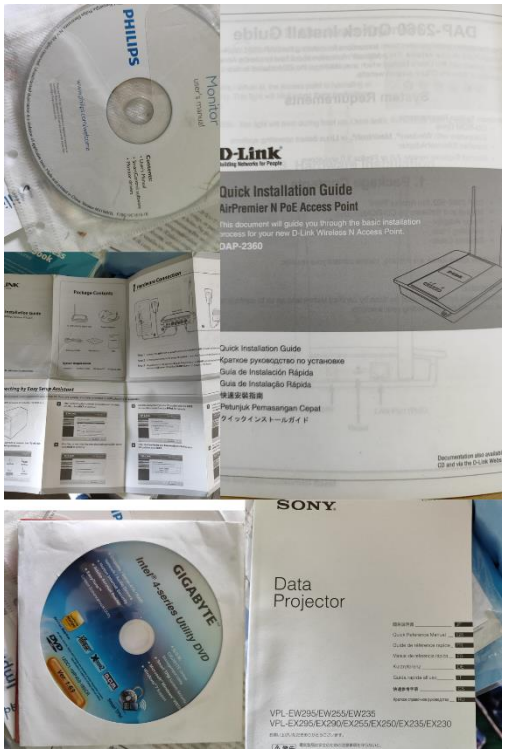

Fig. 36. Recopilación de manuales de usuario de los equipos informáticos.

Fig. 37. Instalación de señalización y extintor en área de Psicología.

Fig. 38. Instalación de señalización y extintor en Dirección.

Fig. 39. Capacitación docente sobre seguridad de la información.

Fig. 40. Capacitación a estudiantes sobre seguridad de la información.

Fig. 41. Aula de Innovación.

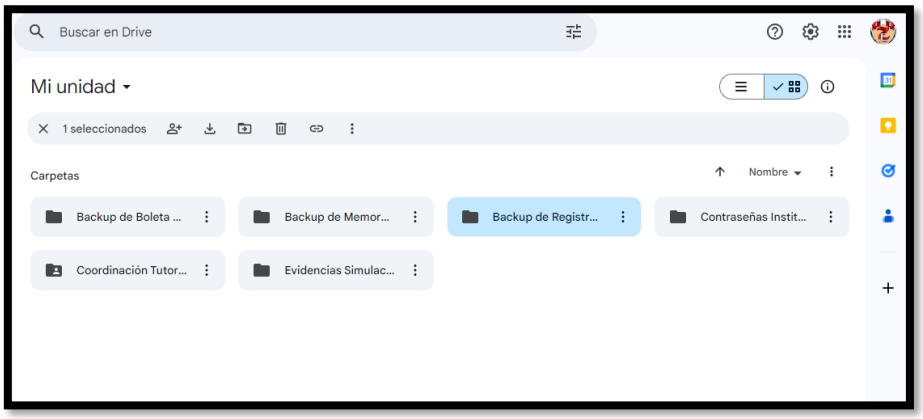

Fig. 42. Almacenamiento de copias de respaldo institucional.

.

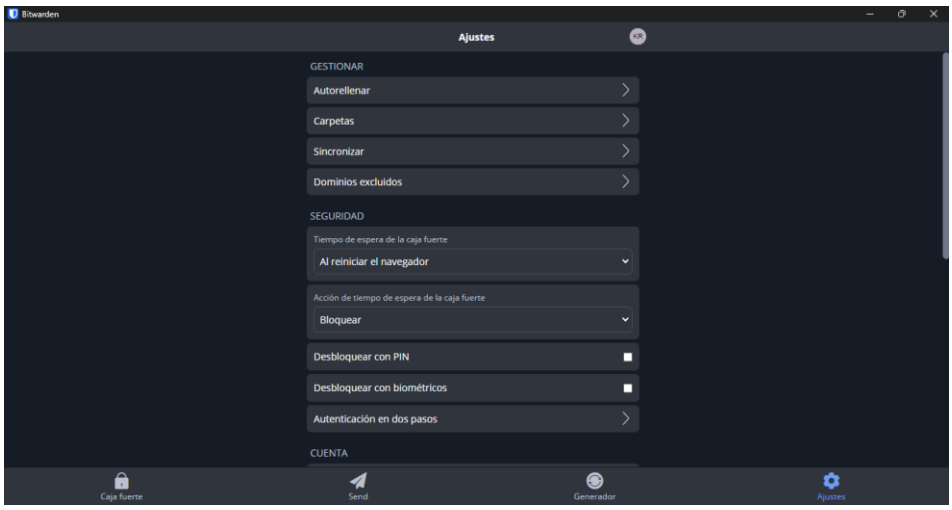

Fig. 43. Herramienta de gestión de contraseñas Bitwarden.

Fig. 44. Capacitación sobre herramienta de gestión de contraseñas Bitwarden.

Fig. 45. Capacitación sobre uso y configuración correcta de los equipos informáticos.

INSTITUCIÓN EDUCATIVA PÚBLICA

"FRANCISCO DE ZELA"

POLÍTICAS Y PROCEDIMIENTOS PARA LA SEGURIDAD DE LA INFORMACIÓN – FRANCISCO DE ZELA

V.1.0

Jr. Rosario N°624 – EL TAMBO

I.E. FRANCISCO DE ZELA	Versión 1.0
	Autor: Mateo Condor Kevin Rolando
	Fecha: 15/02/2024

Política General de la seguridad de la información

1. Resumen

La política de seguridad informática comprende un compromiso de la dirección y de toda la comunidad educativa de la institución educativa "Francisco de Zela" a fin de proteger los activos de información que soportan los procesos de la institución y declaran su apoyo a lograr una correcta implementación del Sistema de Gestión de la Seguridad de la Información basado en la norma ISO/IEC 27001.

2. Introducción

La Institución Educativa "Francisco de Zela" se compromete a proteger la información elaborada, guiando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad y sostenibilidad de las operaciones de la institución. Para ello es importante crear una cultura y concientización de la seguridad de la información en toda la comunidad educativa comenzando por la dirección, coordinadores pedagógicos, docentes, estudiantes, personal administrativo y todo actor que haga uso de los activos informáticos de la institución.

3. Alcance

La totalidad de la información que se genere por parte de los stakeholders de la institución educativa "Francisco de Zela" será en beneficio y mejora de los procesos, siendo de total propiedad de la institución educativa "Francisco de Zela".

4. Objetivos

Asegurar que todos los activos de información integrados dentro de la Institución educativa cuenten con las medidas de seguridad correspondientes.

5. Responsabilidades

- La institución educativa "Francisco de Zela" se compromete a realizar las mejoras necesarias en sus instalaciones físicas con el fin de proteger todos los activos de información que se encuentran dentro de su jurisdicción, garantizando condiciones ambientales y controles de acceso óptimos.
- La institución educativa "Francisco de Zela" procura cumplir con la protección de la información y activos respectivos guiándose de las normativas y leyes vigentes.

6. Principales resultados

- Los principales incidentes que puedan ocurrir en la institución no darán lugar a cortes en los procesos y/o servicios que se brinda.
- Controlar los principales riesgos encontrados en la gestión de riesgos.

7. Políticas relacionadas

- PFZ-P01 - Política General de Gestión de activos
- PFZ-P02 - Política para el uso correcto de la información
- PFZ-P03 - Política para el Acceso físico
- PFZ-P04 - Política de copias de respaldo
- PFZ-P05 - Política de gestión de contraseñas
- PFZ-P06 - Política de uso del internet
- PFZ-P07 - Política de uso de software
- PFZ-P08 - Política de protección contra software malicioso
- PFZ-P09 - Política de escritorio limpio
- PFZ-P010 - Política de capacitación y concientización

I.E. FRANCISCO DE ZELA	Versión 1.0
	Autor: Mateo Condor Kevin Rolando
	Fecha: 15/02/2024

PFZ-P01 - Política General de Gestión de activos

1. Resumen

Los activos de información siempre deben estar gestionados de manera óptima para reducir los riesgos relacionados a este aspecto.

2. Introducción

Todo activo debe formar parte de un inventario especificando diversos detalles necesarios para saber de su uso, propietario encargado y especificaciones.

3. Alcance

Esta política se aplica a los principales activos de información que mantienen los procesos misionales y estratégicos de la institución.

4. Objetivos

Asegurar la gestión adecuada de los activos de información.

5. Responsabilidades

- La dirección de la Institución Educativa “Francisco de Zela” debe asignar un equipo para mantener un inventario actualizado de todos los activos de información, incluyendo detalles como ubicación, propietario, fecha de adquisición, valor y estado de mantenimiento.
- La dirección de la Institución Educativa “Francisco de Zela” debe establecer roles y responsabilidades claros para la gestión de activos, incluyendo la designación de un responsable de activos y un equipo de gestión de activos.
- El Coordinador de Innovación y Soporte Tecnológico (CIST) debe de manera anual: identificar y catalogar todos los activos de información del colegio, incluyendo hardware, software, datos, instalaciones físicas y recursos humanos relacionados con la tecnología.
- Es responsabilidad del Coordinador de Innovación y Soporte Tecnológico (CIST) crear una hoja de vida de cada activo informático para evidenciar toda información referente, boletas de comprar, datos de vencimiento de licencias de SW e historial de mantenimientos preventivos y correctivos.
- Es responsabilidad del Coordinador de Innovación y Soporte Tecnológico (CIST) asignar un número identificatorio a cada equipo portátil que se va a entregar a los docentes y

estudiantes. Por parte de los docentes y estudiantes es su responsabilidad revisar el buen estado del equipo prestado y si no informar de manera inmediata.

- Cuando finalice el término de la jornada laboral el docente o estudiante deberá hacer entrega de los implementos informáticos al CIST para que este a su vez genere una constancia de entrega y haga una revisión del estado, validando lo anterior se procederá a firmar un formato de devolución del activo.
- Los equipos portátiles prestados por ninguna razón serán sacados fuera de la Institución Educativa, si sucede el caso de robo o pérdida se deberá informar al CIST y la Dirección de manera inmediata, adicional a ellos se procederá a poner una denuncia ante la policía.
- Los equipos informáticos asignados son para uso exclusivo de labores de enseñanza y aprendizaje, solo pudiendo almacenar información relevante a la Institución educativa. Será responsabilidad de cada usuario, la eliminación o pérdida de información que no sea referente a la institución.
- Está prohibido intercambiar elementos como mouse, teclados, audífonos, cargadores a los equipos informáticos, si se requiere cambios se debe informar al responsable del activo para su diagnóstico, reparación o reposición.
- Una vez asignado un activo, el usuario es responsable de mantenerlo en buenas condiciones, está prohibido colocar stickers, marcarlos o rayarlos, caso contrario se realizará un descuento aproximado al daño causado.

6. Principales resultados

- Organización adecuada de los activos de información
- Evitar posibles pérdidas de los activos por falta de ubicación asignada
- Evitar posible desligue de responsabilidades por parte de los involucrados responsables.
- Controlar el uso adecuado de los diversos elementos de un activo.

7. Políticas relacionadas

- PFZ-P02 - Política para el uso correcto de la información
- PFZ-P03 - Política para el Acceso físico
- PFZ-P09 - Política de escritorio limpio

I.E. FRANCISCO DE ZELA	Versión 1.0
	Autor: Mateo Condor Kevin Rolando
	Fecha: 15/02/2024

PFZ-P02 - Política para el uso correcto de la información

1. Resumen

Toda información ya sea almacenada o compartida, debe ser protegida de forma segura.

2. Introducción

La información se presenta de manera escrita, de forma digital, almacenada en documentos físicos o electrónicos.

3. Alcance

La política se aplica a todo tipo de información que se utilice o genere en la institución educativa.

4. Objetivos

Asegurar el uso correcto de la información en todos sus tipos de formatos y formas de almacén.

5. Responsabilidades

- Todo personal que acceda a un cargo dentro de la Institución Educativa “Francisco de Zela” debe firmar, adicional a su contrato, un acuerdo de confidencialidad, en el cual se compromete a controlar la no divulgación, uso indebido o sustracción de la información de la institución a la cual tiene acceso.
- Será necesario no entregar ningún tipo de información confidencial por medios electrónicos como celulares, mensajería instantánea, correo electrónico, hasta que no se haya corroborado y verificado la identidad del solicitante.
- La dirección como administrador general de los recursos humanos debe garantizar la confidencialidad de la información de sus docentes, estudiantes y todo personal que trabaja en la institución educativa. Del mismo modo los coordinadores pedagógicos y de tutoría deben salvaguardar toda información dentro de repositorios como Google Drive con una cuenta única y contraseña intransferible.

6. Principales resultados

- Mitigar los riesgos que conllevan entregar información confidencial a terceros.
- Garantizar la confidencialidad de la información de la Institución educativa.

7. Políticas relacionadas

- PFZ-P03 - Política para el Acceso físico

I.E. FRANCISCO DE ZELA	Versión 1.0
	Autor: Mateo Condor Kevin Rolando
	Fecha: 15/02/2024

PFZ-P03 - Política para el Acceso físico

1. Resumen

Todas las áreas en general donde se encuentren almacenados los activos de información deben estar protegidos contra accesos no autorizados, del mismo modo esos accesos se realizarán mediante monitoreo, registrando su entrada y salida respectivamente.

2. Introducción

El acceso no autorizado a puntos restringidos acarrea peligros a la seguridad de la información dentro de la institución educativa.

3. Alcance

La política se relaciona a las áreas de acceso de los activos de información.

4. Objetivos

- Establecer quiénes tienen permiso para ingresar a áreas sensibles donde se encuentran equipos o sistemas críticos.
- Dificultar que personas no autorizadas puedan robar hardware, como computadoras, servidores o dispositivos de almacenamiento.
- Ayudar a prevenir la manipulación no autorizada de equipos, como la instalación de dispositivos de escucha o la alteración de sistemas.

5. Responsabilidades

- Las cámaras de seguridad deben monitorear las principales áreas donde se encuentran los activos de información.
- Todos los visitantes y agentes externos a la Institución deben mostrar un carnet que los identifique y reportar su ingreso con el personal de vigilancia y este a su vez hacer llegar el presente a la Dirección.
- El vigilante encargado de la institución debe siempre velar por la seguridad del local y mantener una constante capacitación.
- Las áreas donde se encuentren los activos que tienen riesgo de incendio deben estar señalizadas. Asimismo, también deben existir señalizaciones para los accesos no autorizados y marcación de las zonas de trabajo.
- Se debe contar con UPS en todos los entornos donde se trabaje con equipos informáticos a fin de evitar riesgos de corte de energía eléctrica.

- Se debe contar con cerraduras de tres puntos en cada área jerárquica.
- Las llaves de cada uno de los salones de clases están a cargo del portero de la institución, siendo él, quien abra las puertas antes del inicio de clases y las mantenga cerradas cuando las clases culminen.
- Las llaves de los ambientes jerárquicos como: Dirección, Coordinación de Letras, Coordinación de Ciencias, Coordinación de Tutoría, Psicología, Aula de Innovación; estarán a cargo del personal designado para cada una de las funciones. El portero deberá tener una copia de las llaves, pero no las usará a menos que sea por pedido expreso de la dirección o del propio encargado, si se usara sin permiso se hará responsable de las respectivas acciones legales.
- Las llaves de los armarios donde se guardan los equipos informáticos, así como los otros armarios con activos importantes solo serán entregadas a los jefes de área y la copia estará a cargo del director de la I.E. Siendo los únicos responsables de la custodia de dichos activos.

6. Principales resultados

- Limitar el acceso solo a personal autorizado, se reduce el riesgo de intrusiones físicas no autorizadas.
- Limitar el acceso a datos sensibles, se reduce el riesgo de robo de información confidencial.
- Controlar quién tiene acceso a los dispositivos y las áreas donde se encuentran, se reduce la posibilidad de que se realicen cambios no autorizados que puedan comprometer la seguridad de la red o los datos.

7. Políticas relacionadas

- PFZ-P02 - Política para el uso correcto de la información.

I.E. FRANCISCO DE ZELA	Versión 1.0
	Autor: Mateo Condor Kevin Rolando
	Fecha: 15/02/2024

PFZ-P04 - Política de copias de respaldo

1. Resumen

Esta política pretende proteger la información almacenada dentro de la institución educativa a fin de preservar la continuidad de los procesos.

2. Introducción

Toda copia de respaldo hará posible la continuidad de los procesos ante posibles perdidas o robo de información relevante para la institución.

3. Alcance

Esta política está relacionada al área de soporte tecnológico de la institución educativa.

4. Objetivos

- Garantizar que la organización pueda seguir funcionando incluso después de un desastre o una pérdida de datos.
- Minimizar el riesgo de sufrir consecuencias catastróficas debido a la pérdida de información importante.

5. Responsabilidades

- El coordinador de innovación y soporte tecnológico (CIST) es el responsable directo de realizar las copias de la información mediante los medios que crea conveniente a fin de salvaguardar todo activo que contenga este tipo de riesgo.
- El coordinador de innovación y soporte tecnológico (CIST) debe tener un inventario de las copias de respaldo que realiza y a su vez reportarlo mediante mesa de partes a la dirección.
- La dirección debe tener todo el inventario de las copias de respaldo realizadas, dentro de las cuales estará: Información de los docentes, estudiantes y personal administrativo; configuraciones de equipos portátiles, carpetas con diferentes archivos de labores realizadas, carpetas con activos de información, contraseñas, repositorios, etc.
- Las copias de seguridad tendrán como objetivo, servir de contingencia para recuperar la información de manera sostenible ante las diferentes amenazas como virus o troyanos, errores de configuración. de los equipos, catástrofes ambientales o industriales, contaminación.

- El responsable de almacenar las copias de seguridad será el CIST a fin de tener el control de acceso, las dos formas de almacenar las copias serán mediante dispositivos de almacenamiento clásico (usb, discos) y mediante un espacio en la nube (Google drive, Onedrive) donde solo personal autorizado tendrá acceso.
- La dirección debe tener en custodia las claves de ingreso al almacenamiento de copias en la nube en caso el CIST no se encuentre disponible y se necesite realizar dicho procedimiento.
- El almacenamiento en la nube de las copias de respaldo será de uso exclusivo, quedando prohibido guardar información que no esté relacionada. Del mismo modo la cuenta usada para este medio será propiedad de la Institución.

6. Principales resultados

- Asegurar que los datos críticos estén disponibles para su recuperación en caso de emergencia.
- Las copias de respaldo actúan como un seguro contra la pérdida de datos debido a errores humanos, fallas de hardware, ataques de malware o desastres naturales.

7. Políticas relacionadas

- PFZ-P01 - Política General de Gestión de activos
- PFZ-P02 - Política para el uso correcto de la información
- PFZ-P09 - Política de escritorio limpio

I.E. FRANCISCO DE ZELA	Versión 1.0
	Autor: Mateo Condor Kevin Rolando
	Fecha: 15/02/2024

PFZ-P05 - Política de gestión de contraseñas

1. Resumen

Una buena gestión de contraseñas asegura que usuarios no autorizados usen de manera inapropiada o con intención maliciosa, equipos informáticos.

2. Introducción

Las contraseñas poco seguras hacen que sea más sencillo ingresar como usuario no autorizado.

3. Alcance

La política se centra en las implementaciones a equipos computacionales dirigidos a personal que labora de manera individual en ellos.

4. Objetivos

- Garantizar que las contraseñas utilizadas por los empleados sean lo suficientemente seguras como para resistir intentos de intrusión.
- Reducir el riesgo de que las cuentas sean comprometidas por accesos no autorizados.

5. Responsabilidades

- Cada usuario que tenga una contraseña asignada es responsable de su buen uso, se evitará compartir el uso de las cuentas, no se deberá dejar en evidencia los datos de acceso que puedan servir para ser usados por otra persona.
- Para el caso de usuarios que utilicen un equipo informático único, se asignará una contraseña por defecto el cual luego debe ser cambiada al primer inicio de sesión teniendo en cuenta:
- Se considera mínimo ocho caracteres.
- La contraseña debe contener: mayúsculas, minúsculas, números y un carácter especial (#, $, %, &).
- No debe existir semejanza entre la contraseña actual y la anterior.
- Las contraseñas deben ser actualizadas cada tres meses a fin de evitar posibles accesos no autorizados. En caso exista un indicio de posible vulnerabilidad se procederá a cambiar la contraseña de manera inmediata.

- Para restablecer una contraseña a un usuario, este debe estar identificado y enviar una solicitud formal mediante mesa de partes.

- El programa para gestionar todas las contraseñas y así evitar que se pierdan o sean olvidadas por los usuarios será: **Bitwarden,** el cual será administrado por el CIST. La dirección, del mismo modo debe tener el acceso a este programa a fin de evitar contratiempos.
- **Bitwarden** también será utilizado por cada usuario que tenga a su cargo una contraseña institucional, siendo su responsabilidad hacer el cambio periódico de la contraseña el cual tiene una interfaz sencilla para poder realizarla sin ningún inconveniente.

6. Principales resultados

- Establecer requisitos mínimos de complejidad para las contraseñas, como longitud, uso de caracteres especiales, letras mayúsculas y minúsculas, y la prohibición de contraseñas comunes o fácilmente adivinables.
- Implementar una política de gestión de contraseñas que incluya rotación periódica de contraseñas y restricciones sobre su uso compartido o almacenamiento

7. Políticas relacionadas

- PFZ-P02 - Política para el uso correcto de la información
- PFZ-P09 - Política de escritorio limpio

I.E. FRANCISCO DE ZELA	Versión 1.0
	Autor: Mateo Condor Kevin Rolando
	Fecha: 15/02/2024

PFZ-P06 - Política de uso del internet

1. Resumen

El acceso a internet es un recurso importante para contribuir a las actividades laborales como accesos a portales del gobierno (SIAGIE, SIMON, SISDORE, etc), portales bancarios entre otros que se necesiten para el cargo desempeñado.

2. Introducción

El uso de internet hoy en día es un aspecto de suma importancia para el trabajo dentro de toda organización.

3. Alcance

Aplicado al área de responsabilidad del CIST de la institución educativa.

4. Objetivos

- Proteger a los estudiantes de contenido inapropiado
- Promover el uso responsable de Internet
- Optimizar el rendimiento académico

5. Responsabilidades

- El acceso a redes sociales está prohibido para los estudiantes en horarios de clases a menos que haya previa coordinación entre el docente y el CIST.
- El acceso a redes sociales solo será permitido para la persona encargada del manejo de marketing de la Institución.
- Los usuarios con acceso a internet, no podrán descargar, copiar o instalar software que necesite licencia de uso, así se evitará sanciones por uso de derechos de autor.
- El CIST debe configurar los niveles de acceso a internet por tipos de usuario (docentes, personal administrativo, estudiantes) bloqueando accesos a sitios web no autorizados e inapropiados, para el caso de permiso especial, siempre deberá ser autorizado e informado de manera oportuna.
- Los usuarios son responsables del uso que apliquen a sus respectivos equipos conectados a internet, será importante controlar los inicios de sesión.
- El usuario que acceda a un sitio no autorizado y provoque un daño al equipo será enteramente responsable de su reparación.

- Está prohibido guardar las credenciales de acceso (contraseñas) cuando los navegadores de internet los soliciten.
- El CIST debe programar horarios de descarga de actualizaciones del sistema en horas que no afecten las labores de la Institución.
- No se debe abrir enlaces que no contenga una conexión segura (HTTPS) a su vez se debe verificar que la URL o enlace debe ser enviado por una persona confiable.
- Todos los usuarios autorizados al uso de internet deben reportar al CIST cualquier situación ocurrida que afecte la seguridad de los activos de información.

6. Principales resultados

- Proteger a los estudiantes de acceder a contenido en línea que pueda ser inapropiado o perjudicial para su desarrollo.
- Educar a los estudiantes sobre el uso responsable de Internet, enseñándoles cómo utilizarlo de manera ética y segura.
- Proporcionar acceso a recursos en línea que complementen el plan de estudios, facilitar la investigación y el aprendizaje colaborativo, así como promover el desarrollo de habilidades digitales necesarias para el éxito en la sociedad actual.

7. Políticas relacionadas

- PFZ-P05 - Política de gestión de contraseñas
- PFZ-P07 - Política de uso de software
- PFZ-P08 - Política de protección contra software malicioso
- PFZ-P010 - Política de capacitación y concientización

I.E. FRANCISCO DE ZELA	Versión 1.0
	Autor: Mateo Condor Kevin Rolando
	Fecha: 15/02/2024

PFZ-P07 - Política de uso de software

1. Resumen

La política se relaciona a uso correcto y formativo del software, entendiendo a este como el medio principal para el uso de las computadoras y del internet.

2. Introducción

El software hoy en día se a convertido en un medio de uso más sencillo de equipos computacionales, teniendo en claro este aspecto, se debe tener especial cuidado en su buen uso a fin de evitar las vulnerabilidades que existen.

3. Alcance

Aplicado al uso de computadoras portátiles y de escritorio, dentro de la institución educativa.

4. Objetivos

- Garantizar el cumplimiento de licencias
- Proteger la seguridad y la integridad de los sistemas
- Promover el uso educativo y productivo del software

5. Responsabilidades

- Queda prohibida la instalación de software sin autorización previa del CIST, esto para evitar piratería e infecciones maliciosas de virus o troyanos que traigan vulnerabilidades a los procesos de la Institución.
- Las licencias de los respectivos Software deben estar inventariados y contener sus soportes de compra y formas de instalación.
- Es responsabilidad del CIST, instalar el software adecuado para uso de cada equipo dentro de la Institución.
- Se debe registrar todo tipo de incidente sucedido con el software, como mantenimientos correctivos, reparaciones o actualizaciones de versión.
- En caso de formateo de los equipos de cómputo, el CIST debe realizar el monitoreo respectivo y suministrar al técnico los medios de instalación, así como las licencias y por ninguna razón permitir que se instalen software pirata sin previa autorización.
- Se instalará para todos los equipos de cómputo el software "**Deep Freeze"** para congelar los discos duros de las máquinas y evitar configuraciones no autorizadas.

6. Principales resultados

- Evitar la piratería de software y asegurarse de que solo se instalen y utilicen programas con licencia legal.
- Incluir restricciones sobre la instalación de software no autorizado, la descarga de programas de fuentes no confiables y la implementación de medidas de seguridad para prevenir la introducción de malware o software malicioso en los sistemas.
- Proporcionar acceso a software que apoye el plan de estudios y las metas educativas del colegio, así como fomentar el aprendizaje de habilidades tecnológicas relevantes para el mundo actual, como la programación, el diseño gráfico, la edición de video, entre otras.
- Evitar error en la configuración de las máquinas e instalación de software no autorizado o ilegal.

7. Políticas relacionadas

- PFZ-P06 - Política de uso del internet

I.E. FRANCISCO DE ZELA	Versión 1.0
	Autor: Mateo Condor Kevin Rolando
	Fecha: 15/02/2024

PFZ-P08 - Política de protección contra software malicioso

1. Resumen

Promover seguridad de uso a los equipos computacionales a fin de evitar riesgos de ataques por virus o malware invasivos y dañinos.

2. Introducción

Hoy en día los ataques de software malicioso se han incrementado de manera drástica gracias al uso masivo de ordenadores en todo el mundo y el acceso a internet para realizar la mayoría de acciones laborales y educativas.

3. Alcance

Aplicado al área encargada al CIST de la institución educativa.

4. Objetivos

- Prevenir infecciones por malware
- Proteger la integridad de los datos
- Garantizar la continuidad de las operaciones

5. Responsabilidades

- Es responsabilidad del CIST velar por la buena gestión de los antivirus y antimalware, asegurando las licencias respectivas para proteger los equipos.
- El CIST debe instalar en cada uno de los equipos el antivirus y antimalware. Aconsejable el antimalware **"Malwarebytes"**.
- Se realizará un monitoreo constante desde la consola del antivirus de las diversas actividades inherentes para lograr reducir los riesgos.
- Cada vez que su use un medio de almacenamiento externo a los equipos como un USB, se debe primero realizar un escaneo con el antivirus para evitar filtraciones de seguridad.
- Los medios de almacenamiento virtual que contengan archivos que pesen más de 300mb quedan prohibidos para su uso.
- Toda sospecha de infección de los equipos debe ser reportado al CIST para su control y monitoreo respectivo, a fin de dar solución a la amenaza.

6. Principales resultados

- Se previene la infiltración y propagación de software malicioso, como virus, troyanos, ransomware y spyware, en los sistemas informáticos del colegio.
- Salvaguardar la integridad y la confidencialidad de los datos almacenados en los sistemas del colegio.
- Se garantiza la continuidad de las operaciones del colegio al minimizar el impacto de posibles ataques de malware.

7. Políticas relacionadas

- PFZ-P04 - Política de copias de respaldo
- PFZ-P05 - Política de gestión de contraseñas
- PFZ-P06 - Política de uso del internet
- PFZ-P07 - Política de uso de software

I.E. FRANCISCO DE ZELA	Versión 1.0
	Autor: Mateo Condor Kevin Rolando
	Fecha: 15/02/2024

PFZ-P09 - Política de escritorio limpio

1. Resumen

Se implementa esta política para aumentar la seguridad física de los activos de información.

2. Introducción

El fin es garantizar que todo tipo de información confidencial y materiales de carácter sensible se mantengan fuera del alcance de personal no autorizado cuando estos no se utilicen.

3. Alcance

La política se aplica de manera conjunta a todo tipo de actor que se encuentre dentro y fuera de la institución educativa.

4. Objetivos

- Fomentar la organización y la eficiencia en el lugar de trabajo.
- Garantizar la seguridad de la información confidencial y sensible.
- Promover una imagen profesional tanto para los empleados como para los visitantes.

5. Responsabilidades

- Todo usuario de los activos debe asegurar la información confidencial dentro de su espacio de trabajo cada vez que termine su horario laboral.
- Los equipos de cómputo deben bloquearse cuando no estén siendo usados por el usuario asignado y apagarse cuando finalice la jornada laboral o de aprendizaje. De igual manera todo equipo que no esté siendo usado debe guardarse en su lugar de almacenamiento.
- Las unidades de almacenamiento como discos externos, USB, que contengan información institucional deben permanecer guardados en un lugar que contenga un seguro con llave cuando no estén siendo utilizados.
- Todo material impreso o fotocopiado debe retirarse de manera inmediata de los dispositivos de impresión y ser entregados al dueño respectivo o almacenarse en archivadores etiquetados de acuerdo a su función.
- Todo documento que contenga información delicada y confidencial debe almacenarse bajo llave en archivadores de metal.
- Las contraseñas no deben estar escritas ni guardadas a la vista de cualquier usuario.

6. Principales resultados

- Se logra mantener el escritorio libre de desorden, archivos innecesarios y objetos no relacionados con el trabajo.
- Reducir el riesgo de dejar documentos confidenciales expuestos, como contraseñas, informes financieros o documentos de clientes, se disminuye la posibilidad de que caigan en manos equivocadas y se comprometa la seguridad.
- Se transmite una impresión positiva de la institución educativa, mostrando un compromiso con la excelencia y el profesionalismo.

7. Políticas relacionadas

- PFZ-P02 - Política para el uso correcto de la información

I.E. FRANCISCO DE ZELA	Versión 1.0
	Autor: Mateo Condor Kevin Rolando
	Fecha: 15/02/2024

PFZ-P010 - Política de capacitación y concientización

1. Resumen

La institución educativa “Francisco de Zela” sabe que, en su gran mayoría las amenazas provienen de las personas ya sea de forma intencionada o por desconocimiento. Es por eso, que un buen plan de capacitación dirigido a todos los usuarios de los activos de información será necesario, para así lograr en cada uno de ellos conciencia de los riesgos de seguridad que conllevan sus actividades.

2. Introducción

Las capacitaciones hoy en día fomentan el aprendizaje y la retroalimentación efectiva del buen uso de las tecnologías de información.

3. Alcance

Esta política se dirige al principal activo que tiene toda organización: “el personal humano”.

4. Objetivos

- Desarrollar habilidades y competencias.
- La política busca concientizar sobre la importancia de la seguridad y el bienestar en el entorno educativo.

5. Responsabilidades

- Toda persona cuya responsabilidad respecto a seguridad de la información sea mayor dentro de la institución educativa, debe recibir una formación óptima, para llevar a cabo las tareas que tengan asignadas.
- La presente política será aplicada a todos los actores dentro de la institución.
- La dirección y el CIST son los responsables de asegurar que todos los miembros de la comunidad educativa reciban formación sobre seguridad de información, antes y durante el desempeño de sus funciones.
- La formación incluirá una concientización sobre seguridad de la información y privacidad, adicionando a ellos, el acceso físico, los principales incidentes que puedan ocurrir, las áreas restringidas a personal autorizado, la forma adecuada de reportar incidentes, formas adecuadas del manejo de computadoras y principales formas de fraude digital o ingeniería social.

- La formación continua de los usuarios será proporcionada a lo largo del año por parte de la Dirección en coordinación con el CIST, fomentando así capacitaciones mensuales sobre temas de importancia.
- De existir cambios significativos en los activos de información como por ejemplo adquisición de nuevas computadoras portátiles, impresoras o cámaras de vigilancia, se proporcionará información actualizada y capacitación de uso adecuado.

6. Principales resultados

- Capacitación en tecnología educativa, pedagogía moderna, manejo de conflictos, liderazgo, entre otros. El objetivo es mejorar la calidad educativa y la efectividad del personal en su rol.
- Se crea un ambiente seguro y saludable para todos los miembros de la comunidad educativa.

7. Políticas relacionadas

- PFZ-P02 - Política para el uso correcto de la información
- PFZ-P04 - Política de copias de respaldo
- PFZ-P05 - Política de gestión de contraseñas
- PFZ-P06 - Política de uso del internet
- PFZ-P07 - Política de uso de software
- PFZ-P08 - Política de protección contra software malicioso